

ON THE FIRST HOMOLOGY OF FINITE INDEX NORMAL SUBGROUPS AND FREE \mathbb{Z}_p -TORUS ACTIONS IN DIMENSION 2 AND 3

LI YU

ABSTRACT. For any finite index normal subgroup N of a finitely presented group G , we obtain some lower bounds of the rank of the first homology of N (with mod p coefficients) in terms of some invariants of G and G/N . Using this, we confirm the Halperin-Carlsson Conjecture for any free \mathbb{Z}_p -torus actions (p is any prime) on 2-dimensional finite CW-complexes and any free \mathbb{Z}_2 -torus actions on compact 3-manifolds.

1. INTRODUCTION

Let $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ be the circle group, and let \mathbb{Z}_p be the additive group $\mathbb{Z}/p\mathbb{Z}$ where p is a prime integer. To avoid confusion, we use \mathbb{F}_p to denote $\mathbb{Z}/p\mathbb{Z}$ as a multiplicative ring (field). For any topological space X , let

$$b_i(X; \mathbb{F}) = \dim_{\mathbb{F}} H_i(X; \mathbb{F}) = \dim_{\mathbb{F}} H^i(X; \mathbb{F}), \quad \forall i \geq 0, \text{ where } \mathbb{F} = \mathbb{F}_p \text{ or } \mathbb{Q}.$$

For any group G , let $b_1(G; \mathbb{F}_p) = \dim_{\mathbb{F}_p} H_1(G; \mathbb{F}_p)$.

Halperin-Carlsson Conjecture: If $G = (\mathbb{Z}_p)^r$ (p is a prime) or $(S^1)^r$ can act freely and continuously on a finite CW-complex X , then we must have $\sum_{i=0}^{\infty} b_i(X; \mathbb{F}_p) \geq 2^r$ or $\sum_{i=0}^{\infty} b_i(X; \mathbb{Q}) \geq 2^r$ respectively.

For convenience, we define

$$\text{hrk}(X; \mathbb{F}) := \sum_{i=0}^{\infty} b_i(X; \mathbb{F}), \text{ where } \mathbb{F} = \mathbb{F}_p \text{ or } \mathbb{Q}.$$

The above conjecture was proposed in the middle of 1980s by S. Halperin in [16] for the torus case, and by G. Carlsson in [9] for the \mathbb{Z}_p -torus case. It is also called *toral rank conjecture* in some literature.

Key words and phrases. Halperin-Carlsson conjecture, \mathbb{Z}_p -torus, free action, fundamental group, 3-manifold, first homology.

2010 *Mathematics Subject Classification.* 57M10, 57R22, 55R91, 57S17, 20C05

The author is partially supported by Natural Science Foundation of China (grant no.11001120) and the PAPD (priority academic program development) of Jiangsu higher education institutions.

In the beginning, this conjecture mainly took the form of whether the existence of a free $(\mathbb{Z}_p)^r$ -action on a product of spheres $S^n \times \cdots \times S^{n_k}$ implies $r \leq k$. Many authors have studied this intriguing conjecture and contributed results with respect to different aspects (see [1, 2, 3, 8, 14, 17]). The reader is referred to see a survey of such results in [4] and [5]. But the general case is still open.

When X is a general finite CW-complex, Halperin-Carlsson Conjecture was proved in [24] for $r \leq 3$ in the torus and \mathbb{Z}_2 -torus cases and $r \leq 2$ in the \mathbb{Z}_p -torus (p is odd prime) case. Some other evidences supporting this conjecture can be found in Cao-Lü [7], Choi-Masuda-Oum [11], Félix-Oprea-Tanré [15], Kamishima-Nakayama [19], Ustinovskii [27] and Yu [28] in various settings.

In many cases where the Halperin-Carlsson Conjecture is confirmed, the multiplicative structure of cohomology plays an essential role in the proof. But we will see that when the dimension of X is 2 or 3, the estimate on $b_1(X; \mathbb{F}_p)$ is often enough for us to prove the lower bound of $\text{hrk}(X; \mathbb{F}_p)$ suggested by the conjecture.

In this paper, we are mainly interested in the Halperin-Carlsson Conjecture for free $(\mathbb{Z}_p)^r$ -actions. Notice that a free action of $(\mathbb{Z}_p)^r$ on an n -dimensional finite CW-complex X may not preserve the cell structure of X . So it is not very clear to the author whether the orbit space of the action is still an n -dimensional CW-complex (or homotopy equivalent to an n -dimensional CW-complex). Since we would like to understand X as a covering space over a not too wild space, we assume that the orbit space $X/(\mathbb{Z}_p)^r$ is still an n -dimensional finite CW-complex. Under this assumption, X can be thought of as a regular $(\mathbb{Z}_p)^r$ -covering space over an n -dimensional finite CW-complex. In addition, we do not assume X is path-connected on priori. The main results of the paper are the following.

Theorem 1.1. *Let K be a 2-dimensional path-connected finite CW-complex. If X is a regular covering space over K with deck transformation group $(\mathbb{Z}_p)^r$ ($r \geq 1$), then $\text{hrk}(X; \mathbb{F}_p) \geq 2^r$. In particular, if X is path connected and $\text{hrk}(X; \mathbb{F}_p) = 2^r$, then r must be 1 or 2 and, X and K must satisfy one of the following conditions:*

- (a) $r = 1$, $H_*(K; \mathbb{F}_p) \cong H_*(X; \mathbb{F}_p) \cong H_*(S^1; \mathbb{F}_p)$,
- (b) $r = 1$, $p = 2$, $H_*(K; \mathbb{F}_2) \cong H_*(\mathbb{R}P^2; \mathbb{F}_2)$, $H_*(X; \mathbb{F}_2) \cong H_*(S^2; \mathbb{F}_2)$.
- (c) $r = 2$, $H_*(K; \mathbb{F}_p) \cong H_*(X; \mathbb{F}_p) \cong H_*(S^1 \times S^1; \mathbb{F}_p)$.

Remark 1.2. All of (a), (b) and (c) can be realized by concrete free $(\mathbb{Z}_p)^r$ -actions on some 2-dimensional CW-complexes X . But these conditions do not determine the homotopy type of K and X . For example,

- when $r = 1$, $p \neq 2$, the K and X in (a) could be both S^1 or Klein bottle;
- when $r = 2$, $p = 2$, the K in (c) may be either $S^1 \times S^1$ or Klein bottle while X is $S^1 \times S^1$.

Problem: Classify all regular $(\mathbb{Z}_p)^r$ -covering spaces X over 2-dimensional finite CW-complexes with $\text{hrk}(X; \mathbb{F}_p) = 2^r$ up to homotopy equivalence.

Theorem 1.3. *If $(\mathbb{Z}_2)^r$ ($r \geq 1$) can act freely on a compact 3-manifold M , then M must satisfy $\text{hrk}(M; \mathbb{F}_2) \geq 2^r$. In particular, if M is closed, connected and $\text{hrk}(M; \mathbb{F}_2) = 2^r$, we must have $r \leq 3$ and, the orbit space $Q = M/(\mathbb{Z}_2)^r$ and M must satisfy one of the following conditions:*

- (a) $r = 1$, $H_*(Q; \mathbb{F}_2) \cong H_*(\mathbb{R}P^3; \mathbb{F}_2)$, $H_*(M; \mathbb{F}_2) \cong H_*(S^3; \mathbb{F}_2)$,
- (b) $r = 2$, $H_*(Q; \mathbb{F}_2) \cong H_*(S^1 \times \mathbb{R}P^2; \mathbb{F}_2)$, $H_*(M; \mathbb{F}_2) \cong H_*(S^1 \times S^2; \mathbb{F}_2)$,
- (c) $r = 3$, $H_*(Q; \mathbb{F}_2) \cong H_*(M; \mathbb{F}_2) \cong H_*(S^1 \times S^1 \times S^1; \mathbb{F}_2)$.

Theorem 1.4. *Suppose $(\mathbb{Z}_p)^r$ ($r \geq 1$) acts freely on a compact manifold M with orbit space $Q = M/(\mathbb{Z}_p)^r$. Assume that the deficiency of the fundamental group of Q is at least 1. Then we must have $b_1(M; \mathbb{F}_p) \geq 2^{r-1}$ and $\text{hrk}(M; \mathbb{F}_p) \geq 2^r$. In particular, if M is connected and $\text{hrk}(M; \mathbb{F}_p) = 2^r$, we must have $r = 1$ or 2 , $p \neq 2$, and M and Q must satisfy one of the following conditions:*

- (a) $r = 1$, $p \neq 2$, $H_*(Q; \mathbb{F}_p) \cong H_*(M; \mathbb{F}_p) \cong H_*(S^1 \times \mathbb{R}P^2; \mathbb{F}_p) \cong H_*(S^1; \mathbb{F}_p)$.
- (b) $r = 2$, $p \neq 2$, $H_*(Q; \mathbb{F}_p) \cong H_*(M; \mathbb{F}_p) \cong H_*(S^1 \times \text{Klein Bottle}; \mathbb{F}_p) \cong H_*(S^1 \times S^1; \mathbb{F}_p)$.

In the settings of Theorem 1.3 and Theorem 1.4, we observe that if $(\mathbb{Z}_p)^r$ ($r \geq 1$) can act freely on a closed connected 3-manifold M with $\text{hrk}(M; \mathbb{F}_p) = 2^r$, the homology groups $H_*(M; \mathbb{F}_p)$ agree with $H_*(S^{n_1} \times \cdots \times S^{n_k}; \mathbb{F}_p)$ for some n_1, \dots, n_k . This motivates us to ask the following question.

Question: If there exists a free $(\mathbb{Z}_p)^r$ -action ($r \geq 1$) on a closed connected manifold M where $\text{hrk}(M; \mathbb{F}_p) = 2^r$, then does $H_*(M; \mathbb{F}_p)$ necessarily agree with $H_*(S^{n_1} \times \cdots \times S^{n_k}; \mathbb{F}_p)$ for some integer n_1, \dots, n_k ?

Note that the dimension of $S^{n_1} \times \cdots \times S^{n_k}$ may be less than the dimension of M when $p \neq 2$. So far, all the examples known to the author (including higher dimensional ones) give positive answer to this question. Moreover, we can strengthen the question by replacing the “closed connected manifold” by “path-connected finite CW-complex” and ask whether the same conclusion holds.

The key piece of machinery used in the proof of all the above results is the following theorem.

Theorem 6.1. Suppose a group G admits finite presentation of deficiency d , i.e. the deficiency of G is at least d . Then for any prime p and any finite index

normal subgroup N of G with $G/N \cong H$,

$$b_1(N; \mathbb{F}_p) \geq 1 + b_1(G; \mathbb{F}_p) \lambda_p^k(H) + d \sum_{j=0}^{k-1} \lambda_p^j(H) - |H|, \quad \forall k \geq 0,$$

where $\lambda_p^k(H) = \dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^k(H) / \Delta_{\mathbb{F}_p}^{k+1}(H)$, $\Delta_{\mathbb{F}_p}(H)$ is the augmentation ideal of the group ring $\mathbb{F}_p[H]$. Note that $b_1(G; \mathbb{F}_p) \geq d$.

In particular, when $H \cong (\mathbb{Z}_p)^r$, we obtain the following results.

Theorem 6.2. Let G be a finitely presentable group with deficiency at least d . Then for any prime p and any normal subgroup N of G with $G/N \cong (\mathbb{Z}_p)^r$,

$$b_1(N; \mathbb{F}_p) \geq 1 + b_1(G; \mathbb{F}_p) |\Omega_{p,r}^k| + d \sum_{j=0}^{k-1} |\Omega_{p,r}^j| - p^r, \quad 0 \leq \forall k \leq r(p-1),$$

where $|\Omega_{p,r}^j|$ is the coefficient of x^j in the polynomial $(1 + x + \cdots + x^{p-1})^r$. In particular, if $G/N \cong (\mathbb{Z}_2)^r$,

$$b_1(N; \mathbb{F}_2) \geq 1 + b_1(G; \mathbb{F}_2) \binom{r}{k} + d \sum_{j=0}^{k-1} \binom{r}{j} - 2^r, \quad 0 \leq \forall k \leq r.$$

Remark 1.5. Indeed, Theorem 6.2 gives us a collection of inequalities, one for each integer k between 0 and $r(p-1)$. In practice, one chooses a proper k to obtain the strongest possible inequality. Theorem 6.1 and Theorem 6.2 ought to be useful for the study of homology growth and subgroup growth of a group.

Remark 1.6. [20, Theorem 1.6] gave another set of lower bounds of $b_1(N; \mathbb{F}_p)$ where N is a normal subgroup of a finitely generated group G with $G/N \cong (\mathbb{Z}_p)^r$. But it seems to the author that Theorem 1.1 and Theorem 1.3 can not be derived from [20, Theorem 1.6].

The paper is organized as follows. In Section 2, we will study finitely presented groups and their presentation complexes. We prove that any finite presentation of a group G can be transformed to another finite presentation of G with some special property. In Section 3, we analyze the cellular structure of a finite-sheeted regular covering space X over a 2-dimensional finite CW-complex K . We will see that the boundary map of the cellular chain complex of X has a rather special form. In Section 4, we will study a special type of square matrices whose rows and columns are indexed by all the elements of an ordered finite group H . In particular, we will study the relations between such matrices and the group ring $\mathbb{F}_p[H]$. In Section 5, we investigate the properties of the family of integers $|\Omega_{p,r}^j|$ and compare them with binomial coefficients. Knowing these properties is very

important for the proof of Theorem 1.1 and Theorem 1.3. In Section 6, we prove Theorem 6.1 and Theorem 6.2. In addition, we will investigate some special cases of Theorem 6.2. In Section 7, we prove Theorem 1.1. In Section 8, we prove Theorem 1.3 and Theorem 1.4. Finally, in Section 9, we use our results to give a new proof of a proposition in [20].

To avoid confusion, we first address some conventions used in this paper.

Conventions:

- The elements of \mathbb{F}_p are treated as integers in some occasions (though they are different from the actual integers). But the meaning should be clear from the context.
- For a set S , we use $|S|$ to denote the number of elements in S .

2. FINITELY PRESENTED GROUPS AND PRESENTATION COMPLEXES

Suppose G be a finitely presentable group. Let $\mathcal{P} = \langle a_1 \cdots, a_n \mid R_1, \cdots, R_m \rangle$ be a finite presentation of G . The integer $n - m$ is called the *deficiency* of \mathcal{P} . When $m = n$, \mathcal{P} is called a *balanced presentation*. The *deficiency* of G is the maximum over all its finite presentations, of the deficiency of each presentation.

Any finite presentation \mathcal{P} canonically determines a 2-dimensional CW-complex $K_{\mathcal{P}}$ called the *presentation complex* of \mathcal{P} .

- $K_{\mathcal{P}}$ has a single vertex q_0 , and one oriented 1-cell γ_j attached to q_0 for each generator a_j ($1 \leq j \leq n$). So the 1-skeleton of $K_{\mathcal{P}}$ is a bouquet of n circles attached to q_0 .
- $K_{\mathcal{P}}$ has one oriented 2-cell β_i for each relator R_i ($1 \leq i \leq m$), where β_i is attached to the 1-skeleton of $K_{\mathcal{P}}$ via a map defined by R_i .

Here, we think of a 1-dimensional CW-complex as a 2-dimensional CW-complex with no 2-cells which corresponds to G being a free group.

Fact: $H_1(G; \mathbb{F}_p) = G/[G, G]G^p \cong H_1(K_{\mathcal{P}}; \mathbb{F}_p)$ for any prime p .

Let $(C_*(K_{\mathcal{P}}; \mathbb{F}_p), \partial_*^{\mathcal{P}})$ be the cellular chain complex of $K_{\mathcal{P}}$ with \mathbb{F}_p -coefficients.

$$0 \longrightarrow C_2(K_{\mathcal{P}}; \mathbb{F}_p) \xrightarrow{\partial_2^{\mathcal{P}}} C_1(K_{\mathcal{P}}; \mathbb{F}_p) \xrightarrow{\partial_1^{\mathcal{P}}} C_0(K_{\mathcal{P}}; \mathbb{F}_p) \longrightarrow 0$$

$$\text{Then } C_1(K_{\mathcal{P}}; \mathbb{F}_p) = \bigoplus_{j=1}^n \langle \gamma_j \rangle, \quad C_2(K_{\mathcal{P}}; \mathbb{F}_p) = \bigoplus_{i=1}^m \langle \beta_i \rangle,$$

where $\langle \gamma_j \rangle$ and $\langle \beta_i \rangle$ are the subspaces of $C_1(K_{\mathcal{P}}; \mathbb{F}_p)$ and $C_2(K_{\mathcal{P}}; \mathbb{F}_p)$ spanned by γ_j and β_i , respectively. The map $\partial_2^{\mathcal{P}}$ can be represented by a matrix $A = (a_{ij})_{n \times m}$,

$a_{ij} \in \mathbb{F}_p$, so that

$$\partial_2^{\mathcal{P}}(\beta_1, \dots, \beta_m) = (\gamma_1, \dots, \gamma_n) \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \cdots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}$$

It is clear that $\dim_{\mathbb{F}_p} \ker(\partial_2^{\mathcal{P}}) = b_2(K_{\mathcal{P}}; \mathbb{F}_p)$ and so $\text{rank}_{\mathbb{F}_p}(A) = m - b_2(K_{\mathcal{P}}; \mathbb{F}_p)$. In addition, by the Euler characteristic of $K_{\mathcal{P}}$, we have:

$$\chi(K_{\mathcal{P}}) = 1 - n + m = 1 - b_1(K_{\mathcal{P}}; \mathbb{F}_p) + b_2(K_{\mathcal{P}}; \mathbb{F}_p).$$

So we get $b_2(K_{\mathcal{P}}; \mathbb{F}_p) = b_1(K_{\mathcal{P}}; \mathbb{F}_p) - n + m$, and so

$$\text{rank}_{\mathbb{F}_p}(A) = n - b_1(K_{\mathcal{P}}; \mathbb{F}_p) = n - b_1(G; \mathbb{F}_p).$$

It is easy to see that we can use two types of elementary transformations to turn A into its *Smith normal form* (we do not require the nonzero entries in the Smith normal form to be $1 \in \mathbb{F}_p$).

Type 1: multiply one row (or column) of A by a nonzero element of \mathbb{F}_p and then add it to another row (or column),

Type 2: switch two rows (or two columns) of A .

In other words, there exists a sequence of elementary transformation matrices P_1, \dots, P_s and Q_1, \dots, Q_t over \mathbb{F}_p so that

$$P_s \cdots P_1 A Q_1 \cdots Q_t = \begin{pmatrix} D & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \quad (1)$$

where D is a diagonal matrix of size $n - b_1(G; \mathbb{F}_p)$ whose diagonals are nonzero elements of \mathbb{F}_p . $P_1, \dots, P_s, Q_1, \dots, Q_t$ are matrices of one of the following forms:

$$T_{ij}(q) = \begin{matrix} & & i & & j & & \\ & & & & & & \\ i & \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \ddots & & \\ j & & q & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix} & & \\ & & & & & & \end{matrix}, \quad q \in \mathbb{F}_p,$$

$$\text{or } S_{ij} = \begin{matrix} & & i & & j & & \\ & & & & & & \\ & & & & & & \\ i & \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & & 1 & \\ & & & \ddots & & \\ j & & 1 & & 0 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix} & & \\ & & & & & & \end{matrix}.$$

Notice that $T_{ij}^{-1}(q) = T_{ij}(-q)$ and $S_{ij}^{-1} = S_{ij}$.

Remark 2.1. In the process of turning A into its Smith normal form, we do not need to multiplies one row (or column) by a nonzero scalar in \mathbb{F}_p since we do not require the nonzero entries in the Smith normal form to be $1 \in \mathbb{F}_p$.

Lemma 2.2. *For any presentation $\mathcal{P} = \langle a_1, \dots, a_n \mid R_1, \dots, R_m \rangle$ of a group G , there exists another presentation $\widehat{\mathcal{P}} = \langle \widehat{a}_1, \dots, \widehat{a}_n \mid \widehat{R}_1, \dots, \widehat{R}_m \rangle$ of G , so that in the cellular chain complex $(C_*(K_{\widehat{\mathcal{P}}}; \mathbb{F}_p), \partial_*^{\widehat{\mathcal{P}}})$ of the presentation complex $K_{\widehat{\mathcal{P}}}$, the boundary map $\partial_2^{\widehat{\mathcal{P}}}$ is represented by $\begin{pmatrix} D & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$ where D is a diagonal matrix of size $n - b_1(G; \mathbb{F}_p)$ whose diagonals are some nonzero elements of \mathbb{F}_p .*

Proof. Denote by $F(a_1, \dots, a_n)$ the free group generated by a_1, \dots, a_n . For a sequence of words $(\omega_1, \dots, \omega_m)$ on a_1, \dots, a_n , let $\langle (\omega_1, \dots, \omega_m) \rangle$ be the normal subgroup of $F(a_1, \dots, a_n)$ generated by $\omega_1, \dots, \omega_m$. For any $T_{ij}(q)$ and S_{ij} , we define

$$(\omega_1, \dots, \omega_m)T_{ij}(q) = (\omega_1, \dots, \omega_{i-1}, \omega_i \omega_j^q, \omega_{i+1}, \dots, \omega_m)$$

$$(\omega_1, \dots, \omega_m)S_{ij} = (\omega_1, \dots, \omega_{i-1}, \omega_j, \omega_{i+1}, \dots, \omega_{j-1}, \omega_i, \omega_{j+1}, \dots, \omega_m)$$

It is easy to see that

$$\langle (\omega_1, \dots, \omega_m)T_{ij}(q) \rangle = \langle (\omega_1, \dots, \omega_m) \rangle = \langle (\omega_1, \dots, \omega_m)S_{ij} \rangle.$$

Next, we return to the discussion of presentation of G and start from (1). Let $(\widetilde{R}_1, \dots, \widetilde{R}_m) = (R_1, \dots, R_m)Q_1 \cdots Q_t$. Then we have a new presentation $\widetilde{\mathcal{P}}$ of G which has the same number of generators and relators as \mathcal{P} .

$$\widetilde{\mathcal{P}} = \langle a_1, \dots, a_n \mid \widetilde{R}_1, \dots, \widetilde{R}_m \rangle \quad (2)$$

Let $K_{\widetilde{\mathcal{P}}}$ be the presentation complex of $\widetilde{\mathcal{P}}$. Then in the cellular chain complex $(C_*(K_{\widetilde{\mathcal{P}}}; \mathbb{F}_p), \partial_*^{\widetilde{\mathcal{P}}})$, the map $\partial_2^{\widetilde{\mathcal{P}}}$ is represented by $AQ_1 \cdots Q_t$.

Moreover, let

$$\begin{aligned}(a'_1, \dots, a'_n) &= (a_1, \dots, a_n)T_{ij}^{-1}(q) = (a_1, \dots, a_n)T_{ij}(-q), \\ (a''_1, \dots, a''_n) &= (a_1, \dots, a_n)S_{ij}^{-1} = (a_1, \dots, a_n)S_{ij}.\end{aligned}$$

$$\text{So by definition, } a'_l = \begin{cases} a_l, & l \neq i; \\ a_i a_j^{-q}, & l = i. \end{cases} \quad a''_l = \begin{cases} a_l, & l \neq i, j; \\ a_j, & l = i; \\ a_i, & l = j. \end{cases}$$

If we replace the generators a_1, \dots, a_n in the presentation (2) by a'_1, \dots, a'_n , replace the a_l ($l \neq i$) occurring in $\tilde{R}_1, \dots, \tilde{R}_m$ by a'_l and replace a_i in $\tilde{R}_1, \dots, \tilde{R}_m$ by $a'_i(a'_j)^q$, we will get a new presentation of G , denoted by

$$\tilde{\mathcal{P}}' = \langle a'_1, \dots, a'_n \mid \tilde{R}'_1, \dots, \tilde{R}'_m \rangle.$$

Similarly, If we replace the generators a_1, \dots, a_n in the presentation (2) by a''_1, \dots, a''_n and change the relators accordingly, we will get a new presentation of G , denoted by

$$\tilde{\mathcal{P}}'' = \langle a''_1, \dots, a''_n \mid \tilde{R}''_1, \dots, \tilde{R}''_m \rangle.$$

Let $K_{\tilde{\mathcal{P}}'}$ and $K_{\tilde{\mathcal{P}}''}$ be the presentation complex of $\tilde{\mathcal{P}}'$ and $\tilde{\mathcal{P}}''$ respectively. Then the boundary map $\partial_2^{\tilde{\mathcal{P}}'}$ and $\partial_2^{\tilde{\mathcal{P}}''}$ in the cellular chain complexes of $K_{\tilde{\mathcal{P}}'}$ and $K_{\tilde{\mathcal{P}}''}$ are represented by $T_{ij}(q)AQ_1 \cdots Q_t$ and $S_{ij}AQ_1 \cdots Q_t$ respectively.

By iterating the above process of transforming the presentation of G according to the matrices P_1, \dots, P_s , we get a new presentation of G , denoted by

$$\hat{\mathcal{P}} = \langle \hat{a}_1, \dots, \hat{a}_n \mid \hat{R}_1, \dots, \hat{R}_m \rangle \quad (3)$$

where the generators $(\hat{a}_1, \dots, \hat{a}_n) = (a_1, \dots, a_n)P_1^{-1} \cdots P_s^{-1}$. Let $K_{\hat{\mathcal{P}}}$ be the presentation complex of $\hat{\mathcal{P}}$. Then in the cellular chain complex $(C_*(K_{\hat{\mathcal{P}}}; \mathbb{F}_p), \partial_*^{\hat{\mathcal{P}}})$ of $K_{\hat{\mathcal{P}}}$, the map $\partial_2^{\hat{\mathcal{P}}}$ is represented by $P_s \cdots P_1 AQ_1 \cdots Q_t$ (see (1)). So the lemma is proved. \square

Remark 2.3. In Lemma 2.2, the two group presentations \mathcal{P} and $\hat{\mathcal{P}}$ of G have the same number of generators and relators. So \mathcal{P} and $\hat{\mathcal{P}}$ have the same deficiency. This fact is important for our proof of Theorem 1.1 and Theorem 1.3 later.

3. INVARIANT CELLULAR STRUCTURES OF REGULAR COVERING SPACES

Let H be a finite group and X be a regular covering space over a 2-dimensional finite CW-complex K with deck transformation H . Let $\xi : X \rightarrow K$ be the covering map. Up to homotopy equivalence, we can assume that K has a single 0-cell q_0 . Let the set of 1-cells of K be $\{\gamma_1, \dots, \gamma_n\}$ and the set of 2-cells of K be

$\{\beta_1, \dots, \beta_m\}$. Then X has a natural cell structure induced from K by ξ which is invariant under the action of H .

Next, we choose

- a point $x_0 \in \xi^{-1}(q_0)$;
- an oriented 1-cell $\tilde{\gamma}_j$ of X attached to x_0 so that $\xi(\tilde{\gamma}_j) = \gamma_j$ ($1 \leq j \leq n$);
- an oriented 2-cell $\tilde{\beta}_i$ of X attached to x_0 so that $\xi(\tilde{\beta}_i) = \beta_i$ ($1 \leq i \leq m$).

Then the sets of 0-cells, 1-cells and 2-cells in X are

- 0-cells : $\{h \cdot x_0 \mid h \in H\}$ denoted by Hx_0 ;
- 1-cells : $\{h \cdot \tilde{\gamma}_j \mid h \in H, 1 \leq j \leq n\}$ denoted by $H\tilde{\gamma}_j$;
- 2-cells : $\{h \cdot \tilde{\beta}_i \mid h \in H, 1 \leq i \leq m\}$ denoted by $H\tilde{\beta}_i$.

We label x_0 , $\tilde{\gamma}_j$ and $\tilde{\beta}_i$ by $e_H \in H$ (the identity of H), and label $h \cdot x_0$, $h \cdot \tilde{\gamma}_j$ and $h \cdot \tilde{\beta}_i$ by h for any $h \in H$. Then every cell σ in X is labeled by a unique element $h_\sigma \in H$ so that $h_{g \cdot \sigma} = gh_\sigma$ for all $g \in H$.

Let $(C_*(X; \mathbb{F}_p), \partial_*^X)$ be the cellular chain complex of X with \mathbb{F}_p -coefficients.

$$0 \longrightarrow C_2(X; \mathbb{F}_p) \xrightarrow{\partial_2^X} C_1(X; \mathbb{F}_p) \xrightarrow{\partial_1^X} C_0(X; \mathbb{F}_p) \longrightarrow 0$$

$$\text{Then } C_1(X; \mathbb{F}_p) = \bigoplus_{j=1}^n \langle H\tilde{\gamma}_j \rangle, \quad C_2(X; \mathbb{F}_p) = \bigoplus_{i=1}^m \langle H\tilde{\beta}_i \rangle$$

where $\langle H\tilde{\gamma}_j \rangle$ and $\langle H\tilde{\beta}_i \rangle$ are the free submodules of $C_1(X; \mathbb{F}_p)$ and $C_2(X; \mathbb{F}_p)$ generated by the set $H\tilde{\gamma}_j$ and $H\tilde{\beta}_i$ over \mathbb{F}_p , respectively. Clearly,

$$\langle H\tilde{\gamma}_j \rangle \cong \langle H\tilde{\beta}_i \rangle \cong \mathbb{F}_p[H],$$

where $\mathbb{F}_p[H]$ is the group ring of H over \mathbb{F}_p .

For the sake of self-containness, we review some basic facts of $\mathbb{F}_p[H]$ below. The group ring $\mathbb{F}_p[H]$ is a free module over \mathbb{F}_p generated by all the elements of H . So we can think of the elements in H forming a basis of $\mathbb{F}_p[H]$ over \mathbb{F}_p , denoted by $\{\delta_h \mid h \in H\}$. Then any element v of $\mathbb{F}_p[H]$ can be written as

$$v = \sum_{h \in H} l_h \delta_h, \quad l_h \in \mathbb{F}_p.$$

Conventions:

- We use e to denote the identity e_H for brevity when there is no ambiguity in the context.
- We use $\hat{0}$ to denote the zero element of $\mathbb{F}_p[H]$ to distinguish it from the scalar $0 \in \mathbb{F}_p$.

The product $*$ on the group ring $\mathbb{F}_p[H]$ is defined by

$$\delta_g * \delta_h := \delta_{gh}, \quad \delta_g * \widehat{0} = \widehat{0}, \quad \forall g, h \in H, \quad k \in \mathbb{F}_p. \quad (4)$$

$$\sum_{g \in H} k_g \delta_g * \sum_{h \in H} l_h \delta_h := \sum_{g \in H} \sum_{h \in H} k_g l_h (\delta_g * \delta_h) = \sum_{g \in H} \sum_{h \in H} k_g l_h \delta_{gh}. \quad (5)$$

The product $*$ is commutative if and only if H itself is commutative.

Notice that $\delta_e * \delta_h = \delta_h * \delta_e = \delta_h$ for all $h \in H$. So δ_e can be identified with the scalar $1 \in \mathbb{F}_p$, and the field \mathbb{F}_p can be embedded in $\mathbb{F}_p[H]$ via the map

$$\begin{aligned} T : \mathbb{F}_p &\longrightarrow \mathbb{F}_p[H] \\ k &\longmapsto k\delta_e \end{aligned}$$

There also exists a canonical homomorphism going the other way, called the *augmentation*. It is the map $\eta_H : \mathbb{F}_p[H] \rightarrow \mathbb{F}_p$, defined by

$$\eta_H \left(\sum_{h \in H} l_h \delta_h \right) = \sum_{h \in H} l_h \in \mathbb{F}_p.$$

The kernel of η_H is called the *augmentation ideal* of $\mathbb{F}_p[H]$, denoted by $\Delta_{\mathbb{F}_p}(H)$. Indeed, $\Delta_{\mathbb{F}_p}(H)$ is a free \mathbb{F}_p -module generated by the set $\{-\delta_e + \delta_h; h \in H\}$ and

$$\mathbb{F}_p[H] = \Delta_{\mathbb{F}_p}(H) \oplus \mathbb{F}_p.$$

The reader is referred to [21] and [22] for more information of group rings and their augmentation ideals.

Remark 3.1. Although we can identify $1 \in \mathbb{F}_p$ with δ_e , we would rather write $-\delta_e + \delta_h \in \Delta_{\mathbb{F}_p}(H)$ instead of $-1 + \delta_h$ in this paper.

There is a natural filtration of $\mathbb{F}_p[H]$ as following.

$$\mathbb{F}_p[H] \supset \Delta_{\mathbb{F}_p}(H) \supset \Delta_{\mathbb{F}_p}^2(H) \supset \cdots \supset \Delta_{\mathbb{F}_p}^k(H) \supset \Delta_{\mathbb{F}_p}^{k+1}(H) \supset \cdots \quad (6)$$

By abuse of notation, let $\Delta_{\mathbb{F}_p}^0(H) := \mathbb{F}_p[H]$. In addition, define

$$\lambda_p^k(H) := \dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^k(H) - \dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^{k+1}(H) = \dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^k(H) / \Delta_{\mathbb{F}_p}^{k+1}(H). \quad (7)$$

So we have

$$\dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^k(H) = \sum_{j \geq k} \lambda_p^j(H) = |H| - \sum_{0 \leq j \leq k-1} \lambda_p^j(H). \quad (8)$$

Since H is a finite group, the filtration (6) becomes stable after finitely many steps. In particular, $\Delta_{\mathbb{F}_p}^k(H) = \{\widehat{0}\}$ for some k if and only if $\Delta_{\mathbb{F}_p}(H)$ is nilpotent. A well known fact (see [13, Theorem 9]) asserts that for any nontrivial group G , the augmentation ideal of the group ring $R[G]$ over a unital ring R is nilpotent if and only if G is a finite p -group and p is nilpotent in R .

Next, let us see what ∂_2^X looks like with respect to the H -invariant cell structure of X . First of all, we choose a total order of all the elements of H , denoted by I , and call (H, I) an *ordered group*. Then we order the basis $\{\delta_h \mid h \in H\}$ of $\mathbb{F}_p[H]$ according to I , too.

Example 1. A total order of elements in $(\mathbb{Z}_2)^3$ is

$$\tilde{0} < e_1 < e_2 < e_3 < e_1 + e_2 < e_1 + e_3 < e_2 + e_3 < e_1 + e_2 + e_3,$$

where $\tilde{0}$ is the additive unit of $(\mathbb{Z}_2)^3$. Then the corresponding ordered basis of $\mathbb{F}_p[(\mathbb{Z}_2)^3]$ is $\delta_{\tilde{0}}, \delta_{e_1}, \delta_{e_2}, \delta_{e_3}, \delta_{e_1+e_2}, \delta_{e_1+e_3}, \delta_{e_2+e_3}, \delta_{e_1+e_2+e_3}$.

Suppose

$$\partial_2^X \tilde{\beta}_i = \sum_{j=1}^n \sum_{s=1}^{d_{ij}} h_{i,s}^j \cdot \tilde{\gamma}_j, \quad 1 \leq i \leq m, \quad h_{i,s}^j \in H, \quad d_{ij} \in \mathbb{Z}_{\geq 0}. \quad (9)$$

Note that d_{ij} may be greater than 1 because the 1-cells in the set $H\tilde{\gamma}_j = \xi^{-1}(\gamma_j)$ may appear more than once in the boundary of a 2-cell $\tilde{\beta}_i$ (see Example 2).

Then for any $g \in H$, we have

$$\partial_2^X(g \cdot \tilde{\beta}_i) = \sum_{j=1}^n \sum_{s=1}^{d_{ij}} (gh_{i,s}^j) \cdot \tilde{\gamma}_j, \quad 1 \leq i \leq m. \quad (10)$$

Next, we order the elements of the sets $H\tilde{\gamma}_j$ and $H\tilde{\beta}_i$ according to the order I on H . Then we get an ordered basis of $C_1(X; \mathbb{F}_p)$ and $C_2(X; \mathbb{F}_p)$, denoted by

$$(H\tilde{\gamma}_1, \dots, H\tilde{\gamma}_n) \text{ and } (H\tilde{\beta}_1, \dots, H\tilde{\beta}_m), \text{ respectively.}$$

Let $\partial_2^X (H\tilde{\beta}_1, \dots, H\tilde{\beta}_m) = (H\tilde{\gamma}_1, \dots, H\tilde{\gamma}_n) \mathbf{M}$, where

$$\mathbf{M} = \begin{pmatrix} \mathbf{M}_{11} & \cdots & \mathbf{M}_{1m} \\ \vdots & \cdots & \vdots \\ \mathbf{M}_{n1} & \cdots & \mathbf{M}_{nm} \end{pmatrix}.$$

Each \mathbf{M}_{ji} ($1 \leq j \leq n, 1 \leq i \leq m$) is a $|H| \times |H|$ matrix which tells us the weight of each 1-cell $h \cdot \tilde{\gamma}_j$ in the boundary of any 2-cell $g \cdot \tilde{\beta}_i$. We prefer to use row vectors in our discussion, so we define

$$\mathbf{B} = \mathbf{M}^t, \quad \mathbf{B}_{ij} = \mathbf{M}_{ji}^t. \quad (11)$$

Note that the rows and columns of each \mathbf{B}_{ij} are both indexed by elements of H in order I . Let $\mathbf{B}_{ij}(g, h) \in \mathbb{F}_p$ denote the entry of \mathbf{B}_{ij} with row index $g \in H$ and column index $h \in H$, and let $\mathbf{B}_{ij}(g)$ be the row of \mathbf{B}_{ij} with index g . We can

identify $\mathbf{B}_{ij}(g)$ with the element $\sum_{h \in H} \mathbf{B}_{ij}(g, h) \delta_h \in \mathbb{F}_p[H]$. Then by (10) and the definition of $*$ (see (5)), we have

$$\mathbf{B}_{ij}(gh) = \delta_g * \mathbf{B}_{ij}(h), \quad \forall g, h \in H. \quad (12)$$

In particular, $\mathbf{B}_{ij}(g) = \delta_g * \mathbf{B}_{ij}(e)$, $\forall g \in H$.

Therefore, all the row vectors of \mathbf{B}_{ij} are determined by only one row $\mathbf{B}_{ij}(e)$. We will see that this is the essential reason why Theorem 1.1 and Theorem 1.3 could hold. To make our discussion convenient, let us introduce the following notion.

Definition 3.2. (Equivariant matrix) Let \mathbf{A} be a $|H| \times |H|$ matrix over \mathbb{F}_p whose rows and columns are indexed by the elements of H in a total order I . We denote by $\mathbf{A}(g, h) \in \mathbb{F}_p$ the entry of \mathbf{A} with row index $g \in H$ and column index $h \in H$, and denote by $\mathbf{A}(g)$ the row vector of \mathbf{A} indexed by $g \in H$. We identify each row $\mathbf{A}(g)$ with the element $\sum_{h \in H} \mathbf{A}(g, h) \delta_h \in \mathbb{F}_p[H]$. We call \mathbf{A} an *equivariant matrix indexed by (H, I)* if $\mathbf{A}(gh) = \delta_g * \mathbf{A}(h)$ for any $g, h \in H$ (see (4) and (5)).

By the above definition, each \mathbf{B}_{ij} in (11) is an equivariant matrix indexed by (H, I) . We will study more properties of this kind of matrices in the next section. Before that, let us see an example of regular covering space from our viewpoint.

Example 2 (Torus). Let X be the 2-dimensional torus

$$T^2 = \{(z_1, z_2) \mid z_i \in \mathbb{C}, |z_i| = 1, i = 1, 2\}.$$

There is a free $(\mathbb{Z}_2)^2 = \langle e_1, e_2 \rangle$ action on X defined by

$$e_1 \cdot (z_1, z_2) = (-z_1, z_2), \quad e_2 \cdot (z_1, z_2) = (z_1, -z_2).$$

It is easy to see that the orbit space $K = X/(\mathbb{Z}_2)^2$ is homeomorphic to T^2 . We can decompose K as the union of one 0-cell q_0 , two 1-cells γ_1, γ_2 and one 2-cell β . The induced $(\mathbb{Z}_2)^2$ -invariant cell decomposition on X and a choice of labeling of cells are shown in Figure 1. There are four 0-cells $(\mathbb{Z}_2)^2 x_0$, eight 1-cells $(\mathbb{Z}_2)^2 \tilde{\gamma}_1$, $(\mathbb{Z}_2)^2 \tilde{\gamma}_2$ and four 2-cells $(\mathbb{Z}_2)^2 \tilde{\beta}$ in X . Choose a total order on $(\mathbb{Z}_2)^2$ to be $\tilde{0} < e_1 < e_2 < e_1 + e_2$, where $\tilde{0}$ is the additive unit of $(\mathbb{Z}_2)^2$. Then the boundary map ∂_2^X is represented by the following matrix.

$$\mathbf{B} = (\mathbf{B}_{11}, \mathbf{B}_{12}) = \begin{matrix} & \begin{matrix} \tilde{0} & e_1 & e_2 & e_1 + e_2 \end{matrix} \\ \begin{matrix} \tilde{0} \\ e_1 \\ e_2 \\ e_1 + e_2 \end{matrix} & \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \end{matrix} \begin{matrix} \tilde{0} & e_1 & e_2 & e_1 + e_2 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{matrix}$$

\mathbf{B}_{11} and \mathbf{B}_{12} are equivariant matrices indexed by $(\mathbb{Z}_2)^2$. They encode the weight of each 1-cell in the boundary of the four 2-cells $(\mathbb{Z}_2)^2 \tilde{\beta}$ in X .

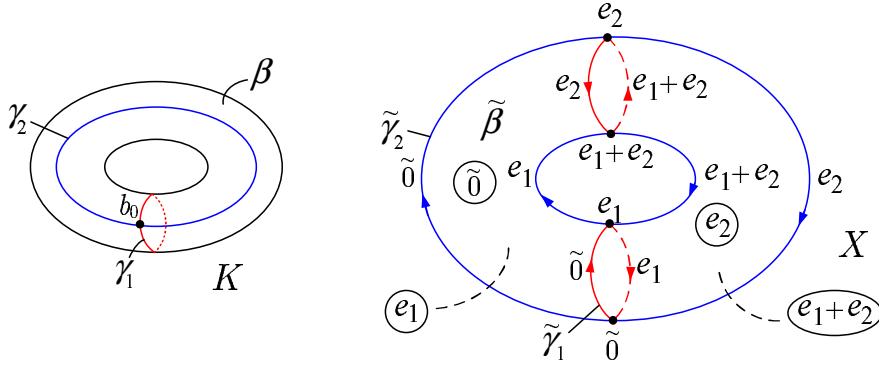


FIGURE 1.

4. PROPERTIES OF EQUIVARIANT MATRICES INDEXED BY AN ORDERED GROUP

Definition 4.1. An element $v \in \mathbb{F}_p[H]$ is called *balanced* if v lies in $\Delta_{\mathbb{F}_p}(H)$, otherwise v is called *unbalanced*. An equivariant matrix \mathbf{A} indexed by an ordered group (H, I) is called *balanced* (or *unbalanced*) if every row of \mathbf{A} is a balanced (or unbalanced) element of $\mathbb{F}_p[H]$.

The following lemma is immediate from our definitions.

Lemma 4.2. For an equivariant matrix \mathbf{A} indexed by an ordered group (H, I) , the following three statements are equivalent.

- (i) \mathbf{A} is balanced (or unbalanced).
- (ii) There exists some $h \in H$ so that $\mathbf{A}(h)$ is balanced (or unbalanced).
- (iii) $\mathbf{A}(e)$ is balanced (or unbalanced).

So all the equivariant matrices indexed by (H, I) are divided into two classes — balanced vs. unbalanced.

In the rest of the paper, we will not distinguish an equivariant matrix \mathbf{A} indexed by an ordered group (H, I) and the linear transformation on $\mathbb{F}_p[H]$ defined by \mathbf{A} with respect to the ordered basis $\{\delta_h \mid h \in H\}$ of $\mathbb{F}_p[H]$. In addition, we think of any $v \in \mathbb{F}_p[H]$ as a row vector and use $v\mathbf{A}$ to denote the image of v under \mathbf{A} .

Lemma 4.3. Let \mathbf{A} be an equivariant matrix indexed by an ordered group (H, I) . Then $v\mathbf{A} = v * \mathbf{A}(e)$ for any $v \in \mathbb{F}_p[H]$.

Proof. Suppose $v = \sum_{h \in H} l_h \delta_h$ where $l_h \in \mathbb{F}_p$. Then

$$v\mathbf{A} = \sum_{h \in H} l_h \mathbf{A}(h) = \sum_{h \in H} l_h (\delta_h * \mathbf{A}(e)) = \left(\sum_{h \in H} l_h \delta_h \right) * \mathbf{A}(e) = v * \mathbf{A}(e).$$

□

Lemma 4.4. *For an equivariant matrix \mathbf{A} indexed by an ordered group (H, I) , the linear map on $\mathbb{F}_p[H]$ defined by \mathbf{A} preserves $\Delta_{\mathbb{F}_p}^k(H)$ for any $k \geq 0$. In particular, when \mathbf{A} is balanced, \mathbf{A} maps $\Delta_{\mathbb{F}_p}^k(H)$ into $\Delta_{\mathbb{F}_p}^{k+1}(H)$ for any $k \geq 0$.*

Proof. Note that $\Delta_{\mathbb{F}_p}^k(H)$ ($k \geq 1$) is linearly spanned by the following set over \mathbb{F}_p

$$\Phi_H^{(k)} := \{(-\delta_e + \delta_{g_1}) * \cdots * (-\delta_e + \delta_{g_k}) \in \mathbb{F}_p[H], \text{ where } g_1, \dots, g_k \in H\} \quad (13)$$

Note that here g_1, \dots, g_k are not necessarily different. For any tuple (g_1, \dots, g_k) of elements in H , let

$$v_{(g_1, \dots, g_k)} := (-\delta_e + \delta_{g_1}) * \cdots * (-\delta_e + \delta_{g_k}), \quad k \geq 1. \quad (14)$$

In particular, $v_{(h)} = -\delta_e + \delta_h$ for any $h \in H$ and $v_{(e)} = \widehat{0}$. By this notation,

$$\Phi_H^{(k)} = \{v_{(g_1, \dots, g_k)} \in \mathbb{F}_p[H]; g_1, \dots, g_k \in H\}, \quad k \geq 1.$$

Let $\mathbf{A}(e) = \sum_{h \in H} l_h \delta_h$, $l_h \in \mathbb{F}_p$. For brevity, let $\|\mathbf{A}(e)\| = \eta_H(\mathbf{A}(e)) \in \mathbb{F}_p$. Then \mathbf{A} is balanced if and only if $\|\mathbf{A}(e)\| = 0 \in \mathbb{F}_p$.

$$\begin{aligned} \mathbf{A}(e) &= \sum_{h \in H} l_h \delta_e + \sum_{h \in H} (-l_h \delta_e + l_h \delta_h) \\ &= \|\mathbf{A}(e)\| \delta_e + \sum_{h \in H} l_h (-\delta_e + \delta_h) = \|\mathbf{A}(e)\| \delta_e + \sum_{h \in H} l_h v_{(h)}. \end{aligned}$$

So for any tuple (g_1, \dots, g_k) of elements in H , we have

$$\begin{aligned} v_{(g_1, \dots, g_k)} \mathbf{A} &= v_{(g_1, \dots, g_k)} * \mathbf{A}(e) = v_{(g_1, \dots, g_k)} * \left(\|\mathbf{A}(e)\| \delta_e + \sum_{h \in H} l_h v_{(h)} \right) \\ &= \|\mathbf{A}(e)\| v_{(g_1, \dots, g_k)} + \sum_{h \in H} l_h v_{(g_1, \dots, g_k, h)}. \end{aligned}$$

Since $v_{(g_1, \dots, g_k)} \in \Delta_{\mathbb{F}_p}^k(H)$, $v_{(g_1, \dots, g_k, h)} \in \Delta_{\mathbb{F}_p}^{k+1}(H) \subset \Delta_{\mathbb{F}_p}^k(H)$, so $v_{(g_1, \dots, g_k)} \mathbf{A} \in \Delta_{\mathbb{F}_p}^k(H)$. This implies that \mathbf{A} preserves $\Delta_{\mathbb{F}_p}^k(H)$.

In particular, when \mathbf{A} is balanced, i.e. $\|\mathbf{A}(e)\| = 0$, we have

$$v_{(g_1, \dots, g_k)} \mathbf{A} = \sum_{h \in H} l_h v_{(g_1, \dots, g_k, h)} \in \Delta_{\mathbb{F}_p}^{k+1}(H).$$

Hence \mathbf{A} maps $\Delta_{\mathbb{F}_p}^k(H)$ into $\Delta_{\mathbb{F}_p}^{k+1}(H)$. The lemma is proved. □

Proposition 4.5. *If \mathbf{A} is a balanced equivariant matrix indexed by an ordered group (H, I) , then $\dim_{\mathbb{F}_p} \ker(\mathbf{A}) \geq \lambda_p^k(H)$ for all $k \geq 0$.*

Proof. By Lemma 4.4, \mathbf{A} maps $\Delta_{\mathbb{F}_p}^k(H)$ into $\Delta_{\mathbb{F}_p}^{k+1}(H)$ for all $k \geq 0$. So we have

$$\dim_{\mathbb{F}_p} \ker(\mathbf{A}) \geq \dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^k(H) - \dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^{k+1}(H) = \lambda_p^k(H).$$

□

In general, $\lambda_p^k(H)$ is not so easy to calculate for an arbitrary finite group H . But when $H = (\mathbb{Z}_p)^r$, the calculation has been done in [18].

Theorem 4.6 (Theorem 3.7 in [18]). *For any $r \geq 1$, $k \geq 0$, $\lambda_p^k((\mathbb{Z}_p)^r)$ equals the coefficient of x^k in the polynomial $(1 + x + \cdots + x^{p-1})^r$.*

In other words, $\lambda_p^k((\mathbb{Z}_p)^r)$ equals the order $|\Omega_{p,r}^k|$ of the following set $\Omega_{p,r}^k$.

$$\Omega_{p,r}^k = \{(j_1, \dots, j_r) \in \mathbb{Z}_{\geq 0}^r \mid j_1 + \cdots + j_r = k, 0 \leq j_i \leq p-1, i = 1, \dots, r\}.$$

Obviously, $|\Omega_{p,r}^k| > 0$ if and only if $0 \leq k \leq r(p-1)$, and we have

$$\sum_{0 \leq k \leq r(p-1)} |\Omega_{p,r}^k| = p^r.$$

In addition, since $(1 + x + \cdots + x^{p-1})^r = (1 - x^p)^r(1 - x)^{-r}$, we get

$$\begin{aligned} |\Omega_{p,r}^k| &= \sum_{0 \leq j \leq \frac{k}{p}} (-1)^{k-(p-1)j} \binom{r}{j} \binom{-r}{k-pj} \\ &= \sum_{0 \leq j \leq \frac{k}{p}} (-1)^j \binom{r}{j} \binom{k-pj+r-1}{k-pj}. \end{aligned} \quad (15)$$

Obviously, $|\Omega_{p,r}^k| \geq |\Omega_{2,r}^k| = \binom{r}{k}$ for any prime p .

In addition, let $\{e_1, \dots, e_r\}$ be a set of additive generators of $(\mathbb{Z}_p)^r$ and let $\tilde{0}$ be the additive unit. Then a basis of $\Delta_{\mathbb{F}_p}^k((\mathbb{Z}_p)^r)$ is given by:

$$\left\{ \overbrace{(-\delta_{\tilde{0}} + \delta_{e_1}) * \cdots * (-\delta_{\tilde{0}} + \delta_{e_1})}^{j_1} * \cdots * \overbrace{(-\delta_{\tilde{0}} + \delta_{e_r}) * \cdots * (-\delta_{\tilde{0}} + \delta_{e_r})}^{j_r} \right\},$$

where (j_1, \dots, j_r) ranges over all the elements of $\bigcup_{m \geq k} \Omega_{p,r}^m$.

Remark 4.7. The augmentation ideal $\Delta((\mathbb{Z}_p)^r)$ of $\mathbb{Z}[(\mathbb{Z}_p)^r]$ is also well studied (see [6, 23, 25, 26]). In particular, $\Delta^k((\mathbb{Z}_p)^r)$'s are all free abelian groups of the same rank. So $\Delta^k((\mathbb{Z}_p)^r)/\Delta^{k+1}((\mathbb{Z}_p)^r)$ is torsion for all $k \geq 1$.

5. PROPERTIES OF $|\Omega_{p,r}^m|$

In this section, we investigate the properties of $|\Omega_{p,r}^j|$'s and compare them with binomial coefficients. Knowing these properties is very important for the proof of Theorem 1.1 and Theorem 1.3.

It is easy to see that $|\Omega_{p,r}^0| = 1$, $|\Omega_{p,r}^1| = r$ for any prime p , and

$$|\Omega_{p,1}^m| = \begin{cases} 1, & 0 \leq m \leq p-1; \\ 0, & \text{otherwise.} \end{cases} \quad (16)$$

Moreover, we have the following recursive relation

$$|\Omega_{p,r}^m| = |\Omega_{p,r-1}^m| + |\Omega_{p,r-1}^{m-1}| + \cdots + |\Omega_{p,r-1}^{m-(p-1)}|, \quad \forall m \in \mathbb{Z}. \quad (17)$$

An easy way to prove this recursive relation is to understand $|\Omega_{p,r}^m|$ as the number of different ways of putting m indistinguishable balls into r different bags where each bag can hold at most $p-1$ balls. If there are exactly i balls in the first bag, then the remaining $m-i$ balls must be put in other $r-1$ bags, which gives the term $|\Omega_{p,r-1}^{m-i}|$ on the right hand side of (17).

When $r = 2$, $|\Omega_{p,2}^m| = |\Omega_{p,1}^m| + |\Omega_{p,1}^{m-1}| + \cdots + |\Omega_{p,1}^{m-(p-1)}|$ for $\forall m \in \mathbb{Z}$. So we get

$$|\Omega_{p,2}^m| = \begin{cases} m+1, & 0 \leq m \leq p-1; \\ 2p-m-1, & p \leq m \leq 2(p-1); \\ 0, & \text{otherwise.} \end{cases} \quad (18)$$

Notice that $|\Omega_{p,2}^m| = |\Omega_{p,2}^{2(p-1)-m}|$ for any $0 \leq m \leq 2(p-1)$, and $|\Omega_{p,2}^m|$ reaches its maximum at $m = p-1$. In general, $|\Omega_{p,r}^m|$ has the following properties which are similar to the properties of binomial coefficients.

Lemma 5.1. *For any prime p and any $0 \leq m \leq r(p-1)$, $r \geq 1$,*

- (i) $|\Omega_{p,r}^m| = |\Omega_{p,r}^{r(p-1)-m}|$;
- (ii) $|\Omega_{p,r}^m| > |\Omega_{p,r}^{m-1}|$ for any $r \geq 2$ and $0 \leq m \leq \lfloor \frac{r(p-1)}{2} \rfloor$;
- (iii) $|\Omega_{p,r-1}^m| > |\Omega_{p,r-1}^{m-p}|$ for any $r \geq 2$ and $\lfloor \frac{r(p-1)}{2} \rfloor \leq m \leq \lfloor \frac{(r+1)(p-1)}{2} \rfloor$.
- (iv) $|\Omega_{p,r}^m|$ reaches its maximum at $m = \lfloor \frac{r(p-1)}{2} \rfloor$.

Proof. There is a bijection between the set $\Omega_{p,r}^m$ and $\Omega_{p,r}^{r(p-1)-m}$ which sends any $(j_1, \dots, j_r) \in \Omega_{p,r}^m$ to $(p-1-j_1, \dots, p-1-j_r) \in \Omega_{p,r}^{r(p-1)-m}$. This proves (i).

The formula (18) implies that (ii) and (iii) holds for $r = 2$. Assume (ii) and (iii) both hold for $r-1$. Then by (17), we have

$$|\Omega_{p,r}^m| - |\Omega_{p,r}^{m-1}| = |\Omega_{p,r-1}^m| - |\Omega_{p,r-1}^{m-p}|. \quad (19)$$

$$|\Omega_{p,r}^m| - |\Omega_{p,r}^{m-p}| = |\Omega_{p,r-1}^m| + \cdots + |\Omega_{p,r-1}^{m-p+1}| - |\Omega_{p,r-1}^{m-p}| - \cdots - |\Omega_{p,r-1}^{m-2p+1}|. \quad (20)$$

If $0 \leq m \leq \lfloor \frac{(r-1)(p-1)}{2} \rfloor$, the induction hypothesis of (ii) and equation (19) imply $|\Omega_{p,r}^m| > |\Omega_{p,r}^{m-1}|$. If $\lfloor \frac{(r-1)(p-1)}{2} \rfloor \leq m \leq \lfloor \frac{r(p-1)}{2} \rfloor$, the induction hypothesis of (iii) and (19) imply $|\Omega_{p,r}^m| > |\Omega_{p,r}^{m-1}|$. So the induction step of (ii) is finished. As for (iii), we observe that when $\lfloor \frac{r(p-1)}{2} \rfloor \leq m \leq \lfloor \frac{(r+1)(p-1)}{2} \rfloor$,

$$m - p - i + 1 < (r-1)(p-1) - (m - p + i), \quad 1 \leq i \leq p$$

- When $(r-1)(p-1) - (m - p + i) \leq \lfloor \frac{(r-1)(p-1)}{2} \rfloor$, i.e. $m - p + i \geq \lfloor \frac{r(p-1)}{2} \rfloor$,

$$|\Omega_{p,r-1}^{m-p+i}| = |\Omega_{p,r-1}^{(r-1)(p-1)-(m-p+i)}| > |\Omega_{p,r-1}^{m-p-i+1}| \quad (\text{by the induction of (ii)}).$$

- When $m - p + i \leq \lfloor \frac{r(p-1)}{2} \rfloor$, since $m - p - i + 1 < m - p + i$,

$$|\Omega_{p,r-1}^{m-p+i}| > |\Omega_{p,r-1}^{m-p-i+1}| \quad (\text{by the induction step of (ii)}).$$

So when $\lfloor \frac{r(p-1)}{2} \rfloor \leq m \leq \lfloor \frac{(r+1)(p-1)}{2} \rfloor$, we have $|\Omega_{p,r-1}^{m-p+i}| > |\Omega_{p,r-1}^{m-p-i+1}|$ for each $1 \leq i \leq p$. Using this, we pair $|\Omega_{p,r-1}^{m-p+i}|$ with $|\Omega_{p,r-1}^{m-p-i+1}|$ in the right hand side of (20) and get

$$|\Omega_{p,r}^m| - |\Omega_{p,r}^{m-p}| = \sum_{1 \leq i \leq p} |\Omega_{p,r-1}^{m-p+i}| - |\Omega_{p,r-1}^{m-p-i+1}| > 0.$$

This finishes the induction step of (iii). Finally, (iv) follows easily from (i)–(iii). So the lemma is proved. \square

To have some idea of how fast $|\Omega_{p,r}^m|$ increases with respect to m , let us compare $|\Omega_{p,r}^m|$ with binomial coefficients. But the formula (15) of $|\Omega_{p,r}^m|$ is an alternating sum, which is not convenient for our purpose. So we give another way to compute $|\Omega_{p,r}^m|$ as following. Let $f(x) = 1 + x + \cdots + x^{p-1}$ and $F(x) = f(x)^r$. Then

$$|\Omega_{p,r}^m| = \frac{F^{(m)}(0)}{m!}$$

where $F^{(m)}(x)$ is the m -th derivative of $F(x)$. To write a concise formula of $F^{(m)}(x)$, let us first introduce some notations. Let $\Theta_{m,p}$ be the set of all partitions of m into positive integers no more than $p-1$. Any element of $\Theta_{m,p}$ can be represented by an integral vector

$$\alpha = (\overbrace{n_1, \dots, n_1}^{l_1}, \overbrace{n_2, \dots, n_2}^{l_2}, \dots, \overbrace{n_s, \dots, n_s}^{l_s}),$$

where $1 \leq n_1 < n_2 < \cdots < n_s \leq p-1$, $l_1, \dots, l_s \geq 1$ and $l_1 n_1 + \cdots + l_s n_s = m$.

$$\text{Define } N_\alpha := (n_1!)^{l_1} (n_2!)^{l_2} \cdots (n_s!)^{l_s}, \quad L_\alpha := l_1! l_2! \cdots l_s!,$$

$$|\alpha| := l_1 + l_2 + \cdots + l_s, \text{ so } 1 \leq |\alpha| \leq m, \text{ and}$$

$$f^{(\alpha)}(x) := (f^{(n_1)}(x))^{l_1} (f^{(n_2)}(x))^{l_2} \cdots (f^{(n_s)}(x))^{l_s},$$

where $f^{(k)}(x)$ is the k -th derivative of $f(x)$. By the fact that $f^{(k)}(x) \equiv 0$ when $k > p - 1$, we can show (by inductively taking the derivative of $F(x)$ using Leibniz's rule)

$$F^{(m)}(x) = \sum_{\alpha \in \Theta_{m,p}} \frac{r!}{(r - |\alpha|)!} (f(x))^{r - |\alpha|} \frac{m!}{N_\alpha L_\alpha} f^{(\alpha)}(x), \quad 1 \leq m \leq r.$$

Since $f^{(k)}(0) = k!$, $1 \leq k \leq p - 1$, we have $f^{(\alpha)}(0) = N_\alpha$. So we get

$$\begin{aligned} F^{(m)}(0) &= \sum_{\alpha \in \Theta_{m,p}} \frac{r!}{(r - |\alpha|)!} \cdot \frac{m!}{L_\alpha}, \quad 1 \leq m \leq r. \\ \implies |\Omega_{p,r}^m| &= \frac{F^{(m)}(0)}{m!} = \sum_{\alpha \in \Theta_{m,p}} \frac{r!}{(r - |\alpha|)!} \cdot \frac{1}{L_\alpha}, \quad 1 \leq m \leq r. \end{aligned} \quad (21)$$

Lemma 5.2. *For any prime p and any $1 \leq m \leq r$,*

$$\frac{|\Omega_{p,r}^m|}{|\Omega_{p,r}^{m-1}|} \geq \frac{|\Omega_{2,r}^m|}{|\Omega_{2,r}^{m-1}|} = \frac{\binom{r}{m}}{\binom{r}{m-1}} = \frac{r - m + 1}{m}.$$

Moreover, the above equality holds only when $m = 1$.

Proof. We can embed $\Theta_{m-1,p}$ into $\Theta_{m,p}$ by mapping $\beta \in \Theta_{m-1,p}$ to $\beta^+ \in \Theta_{m,p}$

$$\beta = (\overbrace{n_1, \dots, n_1}^{l_1}, \dots, \overbrace{n_s, \dots, n_s}^{l_s}) \longmapsto \beta^+ = (1, \overbrace{n_1, \dots, n_1}^{l_1}, \dots, \overbrace{n_s, \dots, n_s}^{l_s}).$$

This map is obviously injective. Note that $|\beta^+| = |\beta| + 1$,

$$L_{\beta^+} = \begin{cases} (l_1 + 1)L_\beta, & n_1 = 1; \\ L_\beta, & n_1 > 1. \end{cases}$$

$$\implies \frac{r!}{(r - |\beta^+|)!} \cdot \frac{1}{L_{\beta^+}} = \begin{cases} \frac{r!}{(r - |\beta| - 1)!} \cdot \frac{1}{(l_1 + 1)L_\beta} = \frac{r - |\beta|}{l_1 + 1} \left(\frac{r!}{(r - |\beta|)!} \cdot \frac{1}{L_\beta} \right), & n_1 = 1; \\ \frac{r!}{(r - |\beta| - 1)!} \cdot \frac{1}{L_\beta} = (r - |\beta|) \left(\frac{r!}{(r - |\beta|)!} \cdot \frac{1}{L_\beta} \right), & n_1 > 1. \end{cases}$$

Since $1 \leq l_1 \leq |\beta| \leq m - 1$, we have $r - |\beta| > \frac{r - |\beta|}{l_1 + 1} \geq \frac{r - m + 1}{m}$. So

$$\frac{r!}{(r - |\beta^+|)!} \cdot \frac{1}{L_{\beta^+}} \geq \frac{r - m + 1}{m} \left(\frac{r!}{(r - |\beta|)!} \cdot \frac{1}{L_\beta} \right), \quad \beta \in \Theta_{m-1,p}.$$

Then by (21), we get

$$\begin{aligned}
|\Omega_{p,r}^m| &= \sum_{\alpha \in \Theta_{m,p}} \frac{r!}{(r-|\alpha|)!} \cdot \frac{1}{L_\alpha} \geq \sum_{\beta \in \Theta_{m-1,p}} \frac{r!}{(r-|\beta^+|)!} \cdot \frac{1}{L_{\beta^+}} \\
&\geq \frac{r-m+1}{m} \cdot \sum_{\beta \in \Theta_{m-1,p}} \frac{r!}{(r-|\beta|)!} \cdot \frac{1}{L_\beta} \\
&\geq \frac{r-m+1}{m} \cdot |\Omega_{p,r}^{m-1}|.
\end{aligned}$$

In particular, when $r \geq m \geq 2$, the partition $(m) \in \Theta_{m,p}$ can not be written as β^+ for any $\beta \in \Theta_{m-1,p}$, which implies $|\Omega_{p,r}^m| > \frac{r-m+1}{m} \cdot |\Omega_{p,r}^{m-1}|$ in the above argument. So if $|\Omega_{p,r}^m| = \frac{r-m+1}{m} \cdot |\Omega_{p,r}^{m-1}|$, m must equal 1. \square

6. LOWER BOUNDS OF THE FIRST HOMOLOGY GROUP OF FINITE INDEX NORMAL SUBGROUPS

In this section, we will prove the following theorem which is the driving force behind the proofs of all the main results of this paper.

Theorem 6.1. *Suppose a group G admits finite presentation of deficiency d , i.e. the deficiency of G is at least d . Then for any prime p and any finite index normal subgroup N of G with $G/N \cong H$,*

$$b_1(N; \mathbb{F}_p) \geq 1 + b_1(G; \mathbb{F}_p) \lambda_p^k(H) + d \sum_{j=0}^{k-1} \lambda_p^j(H) - |H|, \quad \forall k \geq 0,$$

where $\lambda_p^k(H) = \dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^k(H) / \Delta_{\mathbb{F}_p}^{k+1}(H)$, $\Delta_{\mathbb{F}_p}(H)$ is the augmentation ideal of the group ring $\mathbb{F}_p[H]$. Note that $b_1(G; \mathbb{F}_p) \geq d$.

Proof. Let $\mathcal{P} = \langle a_1, \dots, a_n \mid R_1, \dots, R_{n-d} \rangle$ be a deficiency- d presentation of G . Let K be the presentation complex of \mathcal{P} . Then $b_1(K; \mathbb{F}_p) = b_1(G; \mathbb{F}_p)$.

The Euler characteristic of K is

$$\begin{aligned}
\chi(K) &= 1 - b_1(K; \mathbb{F}_p) + b_2(K; \mathbb{F}_p) = 1 - n + (n - d) = 1 - d. \\
\implies b_1(K; \mathbb{F}_p) &= b_2(K; \mathbb{F}_p) + d \geq d, \text{ so } b_1(G; \mathbb{F}_p) \geq d.
\end{aligned}$$

By Lemma 2.2, we can assume that in the cellular chain complex of K ,

$$0 \longrightarrow C_2(K; \mathbb{F}_p) \xrightarrow{\partial_2^K} C_1(K; \mathbb{F}_p) \xrightarrow{\partial_1^K} C_0(K; \mathbb{F}_p) \longrightarrow 0,$$

where the map ∂_2^K is represented by $E = \begin{pmatrix} \mathbf{I}_{n-b_1(G; \mathbb{F}_p)} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$. So all the entries of E are 0 except E_{ii} , $1 \leq i \leq n - b_1(G; \mathbb{F}_p)$.

Let q_0 be the single 0-cell in K and let the set of 1-cells and 2-cells of K be $\{\gamma_1, \dots, \gamma_n\}$ and $\{\beta_1, \dots, \beta_{n-d}\}$.

For a finite index normal subgroup N of G with $G/N \cong H$, let X_N be the covering space of K determined by N . We label the cells of X_N in the same way as we do for X in Section 3. Notice that

$$b_1(X_N; \mathbb{F}_p) = b_1(N; \mathbb{F}_p).$$

In addition, we choose a total order I of the elements of H (the choice of the total order is not essential for our proof).

By the discussion in Section 3, the map $\partial_2^{X_N}$ in the cellular chain complex $(C_*(X_N; \mathbb{F}_p), \partial_*^{X_N})$ is represented by a block matrix \mathbf{B} with respect to the basis $(H\tilde{\gamma}_1, \dots, H\tilde{\gamma}_n)$ and $(H\tilde{\beta}_1, \dots, H\tilde{\beta}_{n-d})$ of $C_1(X_N; \mathbb{F}_p)$ and $C_2(X_N; \mathbb{F}_p)$.

$$\mathbf{B} = \begin{pmatrix} \mathbf{B}_{11} & \mathbf{B}_{12} & \cdots & \mathbf{B}_{1n} \\ \mathbf{B}_{21} & \mathbf{B}_{22} & \cdots & \mathbf{B}_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ \mathbf{B}_{n-d,1} & \mathbf{B}_{n-d,2} & \cdots & \mathbf{B}_{n-d,n} \end{pmatrix}$$

Each block \mathbf{B}_{ij} in \mathbf{B} is an equivariant matrix indexed by the ordered group (H, I) which tells us the weight of each 1-cell $g \cdot \tilde{\gamma}_j$ in the boundary of any 2-cell $h \cdot \tilde{\beta}_i$. Notice that \mathbf{B}_{ij} is balanced if and only if the sum of the weight of all the 1-cells from $H\tilde{\gamma}_j$ in the boundary of the 2-cell $\tilde{\beta}_i$ is a multiple of p , which is equivalent to say $E_{ij} = 0 \in \mathbb{F}_p$. So for any $1 \leq i \leq n-d$, $1 \leq j \leq n$,

$$\mathbf{B}_{ij} \text{ is balanced if and only if } E_{ij} = 0. \quad (22)$$

Now we think of \mathbf{B} as a linear map

$$\mathbf{B} : \overbrace{\mathbb{F}_p[H] \oplus \cdots \oplus \mathbb{F}_p[H]}^{n-d} \longrightarrow \overbrace{\mathbb{F}_p[H] \oplus \cdots \oplus \mathbb{F}_p[H]}^n, \quad (23)$$

where \mathbf{B}_{ij} is a linear map from the i -th copy of $\mathbb{F}_p[H]$ on the left of (23) to the j -th copy of $\mathbb{F}_p[H]$ on the right. Although it is difficult to compute the $\ker(\mathbf{B})$ precisely, we can get some lower bound of $\dim_{\mathbb{F}_p} \ker(\mathbf{B})$ as following.

Note that when \mathbf{B}_{ij} is balanced, it maps $\Delta_{\mathbb{F}_p}^k(H)$ into $\Delta_{\mathbb{F}_p}^{k+1}(H)$; and when \mathbf{B}_{ij} is unbalanced, it still maps $\Delta_{\mathbb{F}_p}^k(H)$ into $\Delta_{\mathbb{F}_p}^k(H)$ for all $k \geq 0$ (see Lemma 4.4). And by (22) and our assumption on E , \mathbf{B}_{ii} ($1 \leq i \leq n-b_1(G; \mathbb{F}_p)$) is unbalanced while all other \mathbf{B}_{ij} 's are balanced. So in particular,

$$\mathbf{B}_{ij} \text{ is balanced, } 1 \leq i \leq n-d, n-b_1(G; \mathbb{F}_p)+1 \leq j \leq n. \quad (24)$$

We claim that: for all $k \geq 0$,

$$\overbrace{\Delta_{\mathbb{F}_p}^k(H) \oplus \cdots \oplus \Delta_{\mathbb{F}_p}^k(H)}^{n-d} \xrightarrow{\mathbf{B}} \overbrace{\Delta_{\mathbb{F}_p}^k(H) \oplus \cdots \oplus \Delta_{\mathbb{F}_p}^k(H)}^{n-b_1(G; \mathbb{F}_p)} \oplus \overbrace{\Delta_{\mathbb{F}_p}^{k+1}(H) \oplus \cdots \oplus \Delta_{\mathbb{F}_p}^{k+1}(H)}^{b_1(G; \mathbb{F}_p)}. \quad (25)$$

Indeed, for any $v_1, \dots, v_{n-d} \in \Delta_{\mathbb{F}_p}^k(H)$, the image of (v_1, \dots, v_{n-d}) under \mathbf{B} is

$$(v_1, \dots, v_{n-d})\mathbf{B} = \left(\sum_{i=1}^{n-d} v_i \mathbf{B}_{i1}, \dots, \sum_{i=1}^{n-d} v_i \mathbf{B}_{in} \right).$$

By Lemma 4.4, each $v_i \mathbf{B}_{ij}$ belongs to $\Delta_{\mathbb{F}_p}^k(H)$. In particular, (24) implies

$$v_i \mathbf{B}_{ij} \in \Delta_{\mathbb{F}_p}^{k+1}(H), \quad 1 \leq i \leq n-d, \quad n-b_1(G; \mathbb{F}_p) + 1 \leq j \leq n.$$

So $\sum_{i=1}^{n-d} v_i \mathbf{B}_{ij} \in \Delta_{\mathbb{F}_p}^{k+1}(H)$, $n-b_1(G; \mathbb{F}_p) + 1 \leq j \leq n$, which prove the claim.

From (25), we can get the following inequality for each $k \geq 0$.

$$\begin{aligned} b_2(X_N; \mathbb{F}_p) &= \dim_{\mathbb{F}_p} \ker(\mathbf{B}) \\ &\geq (b_1(G; \mathbb{F}_p) - d) \dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^k(H) - b_1(G; \mathbb{F}_p) \dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^{k+1}(H). \end{aligned} \quad (26)$$

In addition, the Euler characteristic of X_N is

$$\begin{aligned} \chi(X_N) &= 1 - b_1(X_N; \mathbb{F}_p) + b_2(X_N; \mathbb{F}_p) = |H| \cdot \chi(K) = (1-d)|H|. \\ \implies b_1(N; \mathbb{F}_p) &= b_1(X_N; \mathbb{F}_p) = 1 + b_2(X_N; \mathbb{F}_p) + (d-1)|H|. \end{aligned} \quad (27)$$

Plugging (26) into (27), we get

$$\begin{aligned} b_1(N; \mathbb{F}_p) &\geq 1 + (b_1(G; \mathbb{F}_p) - d) \dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^k(H) - b_1(G; \mathbb{F}_p) \dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^{k+1}(H) + (d-1)|H|. \\ &\geq 1 + b_1(G; \mathbb{F}_p) \left(\dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^k(H) - \dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^{k+1}(H) \right) - d \cdot \dim_{\mathbb{F}_p} \Delta_{\mathbb{F}_p}^k(H) + (d-1)|H| \\ &\geq 1 + b_1(G; \mathbb{F}_p) \lambda_p^k(H) - d \left(|H| - \sum_{0 \leq j \leq k-1} \lambda_p^j(H) \right) + (d-1)|H| \quad (\text{see (8)}) \\ &\geq 1 + b_1(G; \mathbb{F}_p) \lambda_p^k(H) + d \sum_{0 \leq j \leq k-1} \lambda_p^j(H) - |H|. \end{aligned}$$

□

When $H = (\mathbb{Z}_p)^r$, Theorem 6.1 and Theorem 4.6 together imply the following.

Theorem 6.2. *Let G be a finitely presentable group with deficiency at least d . Then for any prime p and any normal subgroup N of G with $G/N \cong (\mathbb{Z}_p)^r$,*

$$b_1(N; \mathbb{F}_p) \geq 1 + b_1(G; \mathbb{F}_p)|\Omega_{p,r}^k| + d \sum_{j=0}^{k-1} |\Omega_{p,r}^j| - p^r, \quad 0 \leq \forall k \leq r(p-1),$$

where $|\Omega_{p,r}^j|$ is the coefficient of x^j in the polynomial $(1 + x + \cdots + x^{p-1})^r$. In particular, if $G/N \cong (\mathbb{Z}_2)^r$,

$$b_1(N; \mathbb{F}_2) \geq 1 + b_1(G; \mathbb{F}_2) \binom{r}{k} + d \sum_{j=0}^{k-1} \binom{r}{j} - 2^r, \quad 0 \leq \forall k \leq r.$$

To have more quantitative idea of the lower bounds of $b_1(N, \mathbb{F}_p)$ in Theorem 6.2, let us investigate two special cases below.

Theorem 6.3. *Let G be a finitely presentable group with deficiency at least 1. Then for any normal subgroup N of G with $G/N \cong (\mathbb{Z}_p)^r$, $r \geq 1$,*

$$b_1(N; \mathbb{F}_p) \geq 2^{r-1}.$$

In particular, if $b_1(N; \mathbb{F}_p) = 2^{r-1}$, we must have $b_1(G; \mathbb{F}_p) = r = 1$ or 2.

Proof. Set $d = 1$ in Theorem 6.2, we have for any $0 \leq k \leq r(p-1)$,

$$\begin{aligned} b_1(N; \mathbb{F}_p) &\geq 1 + b_1(G; \mathbb{F}_p)|\Omega_{p,r}^k| + \sum_{i=0}^{k-1} |\Omega_{p,r}^i| - p^r \\ &\geq 1 + (b_1(G; \mathbb{F}_p) - 1)|\Omega_{p,r}^k| + \sum_{i=0}^k |\Omega_{p,r}^i| - p^r \\ &\geq 1 + (r-1)|\Omega_{p,r}^k| - \sum_{i=k+1}^{r(p-1)} |\Omega_{p,r}^i|. \end{aligned} \tag{28}$$

To prove $b_1(N; \mathbb{F}_p) \geq 2^{r-1}$, we need to show that there exists some $0 \leq k \leq r(p-1)$ so that

$$\Pi_{p,r}^k := (r-1)|\Omega_{p,r}^k| - \sum_{i=k+1}^{r(p-1)} |\Omega_{p,r}^i| \geq 2^{r-1} - 1.$$

Claim 1: $\Pi_{p,r}^{r(p-1)-j} \geq \Pi_{2,r}^{r-j}$ for any prime $p \geq 2$ and $0 \leq j \leq \lceil \frac{r+1}{2} \rceil$, and the equality holds only when $p = 2$ or $j = 1$.

The claim is trivial when $p = 2$. When $p > 2$, by Lemma 5.1 (i),

$$\begin{aligned}\Pi_{p,r}^{r(p-1)-j} &= (r-1)|\Omega_{p,r}^j| - \sum_{i=0}^{j-1} |\Omega_{p,r}^i|, \\ \Pi_{2,r}^{r-j} &= (r-1)|\Omega_{2,r}^j| - \sum_{i=0}^{j-1} |\Omega_{2,r}^i|.\end{aligned}$$

Note that $|\Omega_{p,r}^0| = 1$ for all prime p , so we have

$$\Pi_{p,r}^{r(p-1)-j} - \Pi_{2,r}^{r-j} = (r-1)(|\Omega_{p,r}^j| - |\Omega_{2,r}^j|) - \sum_{i=1}^{j-1} (|\Omega_{p,r}^i| - |\Omega_{2,r}^i|)$$

Moreover, Lemma 5.2 implies that for each $0 \leq i < j \leq \lceil \frac{r+1}{2} \rceil$,

$$k_j := \frac{|\Omega_{p,r}^j|}{|\Omega_{2,r}^j|} \geq \frac{|\Omega_{p,r}^i|}{|\Omega_{2,r}^i|} := k_i \geq 1 \quad (\text{the equality holds only when } j = 1).$$

$$\begin{aligned}\text{So } \Pi_{p,r}^{r(p-1)-j} - \Pi_{2,r}^{r-j} &= (k_j - 1)(r-1)|\Omega_{2,r}^j| - \sum_{i=1}^{j-1} (k_i - 1)|\Omega_{2,r}^i| \\ &\geq (k_j - 1) \left((r-1)|\Omega_{2,r}^j| - \sum_{i=1}^{j-1} |\Omega_{2,r}^i| \right) \geq 0\end{aligned}$$

The last “ \geq ” is because $|\Omega_{2,r}^j| \geq |\Omega_{2,r}^i|$ when $1 \leq i < j \leq \lceil \frac{r+1}{2} \rceil$.

Claim 2: For a fixed $r \geq 1$, $\Pi_{2,r}^k$ reaches the maximum only at $k = \lceil \frac{r+1}{2} \rceil$.

Indeed, since $|\Omega_{2,r}^k| = \binom{r}{k}$, $\Pi_{2,r}^k - \Pi_{2,r}^{k-1} = r\binom{r}{k} - (r-1)\binom{r}{k-1}$. So

$$\Pi_{2,r}^k - \Pi_{2,r}^{k-1} > 0 \iff \frac{r\binom{r}{k}}{(r-1)\binom{r}{k-1}} = \frac{r(r-k+1)}{(r-1)k} > 1 \iff k < \frac{r(r+1)}{2r-1}.$$

So when $k \leq \lceil \frac{r+1}{2} \rceil$, $\Pi_{2,r}^k - \Pi_{2,r}^{k-1} > 0$. Similarly, we can show when $k \geq \lceil \frac{r+1}{2} \rceil + 1$, $\Pi_{2,r}^k - \Pi_{2,r}^{k-1} < 0$. Therefore, $\Pi_{2,r}^k$ reaches the maximum at and only at $k = \lceil \frac{r+1}{2} \rceil$. The Claim 2 is proved.

By the above two claims, we have $\Pi_{p,r}^{r(p-1)-\lceil \frac{r+1}{2} \rceil} \geq \Pi_{2,r}^{\lceil \frac{r+1}{2} \rceil}$. Next, we show that

$$\Pi_{2,r}^{\lceil \frac{r+1}{2} \rceil} = (r-1) \binom{r}{\lceil \frac{r+1}{2} \rceil} - \sum_{i=\lceil \frac{r+1}{2} \rceil+1}^r \binom{r}{i} \geq 2^{r-1} - 1, \quad \text{for } \forall r \geq 1. \quad (29)$$

- when $r = 2t + 1$, $t \geq 0$, $\lfloor \frac{r+1}{2} \rfloor = t + 1$,

$$\Pi_{2,r}^{\lfloor \frac{r+1}{2} \rfloor} = 2t \binom{2t+1}{t+1} - \sum_{j=t+2}^{2t+1} \binom{2t+1}{j} = (2t+1) \binom{2t+1}{t+1} - 2^{2t}.$$

So to prove $\Pi_{2,r}^{\lfloor \frac{r+1}{2} \rfloor} \geq 2^{r-1} - 1 = 2^{2t} - 1$, it is enough to prove

$$(2t+1) \binom{2t+1}{t+1} \geq 2^{2t+1} - 1, \quad \forall t \geq 0. \quad (30)$$

- When $r = 2t$, $t \geq 1$, $\lfloor \frac{r+1}{2} \rfloor = t$,

$$\Pi_{2,r}^{\lfloor \frac{r+1}{2} \rfloor} = (2t-1) \binom{2t}{t} - \sum_{i=t+1}^{2t} \binom{2t}{i} = (2t - \frac{1}{2}) \binom{2t}{t} - 2^{2t-1}.$$

So to prove $\Pi_{2,r}^{\lfloor \frac{r+1}{2} \rfloor} \geq 2^{r-1} - 1 = 2^{2t-1} - 1$, it is enough to prove

$$(2t - \frac{1}{2}) \binom{2t}{t} \geq 2^{2t} - 1, \quad \forall t \geq 1. \quad (31)$$

It is an elementary exercise to verify (30) and (31), so we leave it to the reader. In particular, we find that

- if the equality in (30) holds, t must be 0, hence $r = 1$.
- if the equality in (31) holds, t must be 1, hence $r = 2$.

So when the equality $b_1(N; \mathbb{F}_p) = 2^{r-1}$ holds, the inequality in (28) implies that $b_1(G; \mathbb{F}_p) = r = 1$ or 2 . The theorem is proved. \square

Notice that $\binom{r}{\lfloor \frac{r+1}{2} \rfloor} = \binom{r}{\lfloor \frac{r}{2} \rfloor}$. So (29) is equivalent to the following inequality

$$r \binom{r}{\lfloor \frac{r}{2} \rfloor} \geq 2^{r-1} + \sum_{i=\lfloor \frac{r+1}{2} \rfloor}^r \binom{r}{i} - 1, \quad \forall r \geq 1, \quad (32)$$

where the equality holds only when $r = 1$ or 2 .

Theorem 6.4. *Suppose a group G admits a balanced finite presentation. Then for any normal subgroup N of G with $G/N \cong (\mathbb{Z}_p)^r$, $b_1(N; \mathbb{F}_p) \geq 1 + r|\Omega_{p,r}^{\lfloor \frac{r(p-1)}{2} \rfloor}| - p^r$. In particular when the equality holds, we must have $b_1(G; \mathbb{F}_p) = r$.*

Proof. Set $d = 0$ in Theorem 6.2, we get for any $0 \leq k \leq r(p-1)$,

$$b_1(N; \mathbb{F}_p) \geq 1 + b_1(G; \mathbb{F}_p)|\Omega_{p,r}^k| - p^r \geq 1 + r|\Omega_{p,r}^k| - p^r,$$

In addition, by Lemma 5.1 (iv), $|\Omega_{p,r}^k|$ reaches its maximum at $\lfloor \frac{r(p-1)}{2} \rfloor$. \square

7. PROOF OF THEOREM 1.1

Suppose K is a 2-dimensional path-connected CW-complex with finitely many cells and $\xi : X \rightarrow K$ is a regular covering space whose deck transformation group is $(\mathbb{Z}_p)^r$, $r \geq 1$.

Up to homotopy equivalence, we may assume that K has a single 0-cell q_0 . Let the set of 1-cells of K be $\{\gamma_1, \dots, \gamma_n\}$ and the set of 2-cells of K be $\{\beta_1, \dots, \beta_m\}$. We will use the same notations and labels for the cells of X as in Section 3. Note that $b_1(K; \mathbb{F}_p) = b_1(\pi_1(K, q_0); \mathbb{F}_p)$ and $b_1(X; \mathbb{F}_p) = b_1(\pi_1(X, x_0); \mathbb{F}_p)$.

7.1. When X is path connected.

When X is path connected, $b_0(X; \mathbb{F}_p) = 1$ and we must have

$$b_1(K; \mathbb{F}_p) \geq r \geq 1.$$

Note that the fundamental group $\pi_1(K, q_0)$ of K has a natural presentation \mathcal{P}^K defined by the cellular structure of K so that K is the presentation complex of \mathcal{P}^K . The deficiency of \mathcal{P}^K is $n - m$. In addition, since $\xi_* : \pi_1(X, x_0) \rightarrow \pi_1(K, q_0)$ is a monomorphism, we can identify $\pi_1(X, x_0)$ with its image $\xi_*(\pi_1(X, x_0))$. In the rest, we think of $\pi_1(X, x_0)$ as a normal subgroup of $\pi_1(K, q_0)$, and so we have

$$\pi_1(K, q_0)/\pi_1(X, x_0) \cong (\mathbb{Z}_p)^r.$$

This allows us to use the theorems in section 6 to estimate $b_1(\pi_1(X, x_0); \mathbb{F}_p)$.

The Euler characteristic of K and X are

$$\chi(K) = 1 - b_1(K; \mathbb{F}_p) + b_2(K; \mathbb{F}_p) = m - n + 1, \quad (33)$$

$$\chi(X) = 1 - b_1(X; \mathbb{F}_p) + b_2(X; \mathbb{F}_p) = p^r \chi(K). \quad (34)$$

Case 1: When $\chi(K) \leq -1$, $\chi(X) \leq -p^r$. This implies

$$b_1(X; \mathbb{F}_p) \geq p^r + b_2(X; \mathbb{F}_p) + 1.$$

So $\text{hrk}(X; \mathbb{F}_p) = 1 + b_1(X; \mathbb{F}_p) + b_2(X; \mathbb{F}_p) \geq 2b_2(X; \mathbb{F}_p) + p^r + 2 \geq p^r + 2$. So in this case, $\text{hrk}(X; \mathbb{F}_p)$ must be strictly greater than 2^r .

Case 2: When $\chi(K) = 0$, we get $m = n - 1$, $\chi(X) = 0$ and $b_1(X; \mathbb{F}_p) = 1 + b_2(X; \mathbb{F}_p)$. So the natural presentation \mathcal{P}^K of $\pi_1(K, q_0)$ has deficiency 1. Then Theorem 6.3 implies $b_1(X; \mathbb{F}_p) = b_1(\pi_1(X, x_0); \mathbb{F}_p) \geq 2^{r-1}$. So we get

$$\text{hrk}(X; \mathbb{F}_p) = 1 + b_1(X; \mathbb{F}_p) + b_2(X; \mathbb{F}_p) = 2b_1(X; \mathbb{F}_p) \geq 2^r.$$

Moreover, when $\text{hrk}(X; \mathbb{F}_p) = 2^r$, we have $b_1(X; \mathbb{F}_p) = 2^{r-1}$. So Theorem 6.3 implies that $b_1(K; \mathbb{F}_p) = r = 1$ or 2 , and we must have:

- $b_1(K; \mathbb{F}_p) = r = 1, b_2(K; \mathbb{F}_p) = 0, b_1(X; \mathbb{F}_p) = 1, b_2(X; \mathbb{F}_p) = 0$. Then

$$H_*(K; \mathbb{F}_p) \cong H_*(X; \mathbb{F}_p) \cong H_*(S^1; \mathbb{F}_p).$$

- $b_1(K; \mathbb{F}_p) = r = 2, b_2(K; \mathbb{F}_p) = 1, b_1(X; \mathbb{F}_p) = 2, b_2(X; \mathbb{F}_p) = 1$. Then

$$H_*(K; \mathbb{F}_p) \cong H_*(X; \mathbb{F}_p) \cong H_*(S^1 \times S^1; \mathbb{F}_p).$$

Case 3: When $\chi(K) \geq 1$,

$$\text{hrk}(X; \mathbb{F}_p) = \chi(X) + 2b_1(X; \mathbb{F}_p) = p^r \chi(K) + 2b_1(X; \mathbb{F}_p) \geq p^r \geq 2^r.$$

In particular, if $\text{hrk}(X; \mathbb{F}_p) = 2^r$, we must have

$$p = 2, \quad \chi(K) = 1, \quad b_1(X; \mathbb{F}_2) = 0.$$

Then (33) and (34) implies $m = n$ and $b_2(X; \mathbb{F}_2) = 2^r - 1$. So the natural presentation \mathcal{P}^K of $\pi_1(K, q_0)$ has deficiency 0. Then by Theorem 6.4, we get

$$\begin{aligned} b_1(X; \mathbb{F}_2) &= b_1(\pi_1(X, x_0); \mathbb{F}_2) \geq 1 + r|\Omega_{2,r}^{[\frac{r}{2}]}| - 2^r = 1 + r \binom{r}{[\frac{r}{2}]} - 2^r \\ &\quad (\text{by (32)}) \geq \sum_{i=[\frac{r+1}{2}]}^r \binom{r}{i} - 2^{r-1} \geq 0. \end{aligned}$$

- The first inequality holds only when $b_1(K; \mathbb{F}_2) = r$;
- The second inequality holds only when $r = 1$ or 2 (see (32));
- The third inequality holds only when r is odd.

So if $b_1(X; \mathbb{F}_2) = 0$, we must have $b_1(K; \mathbb{F}_2) = r = 1$, and $b_2(X; \mathbb{F}_2) = 1$. In this case,

$$p = 2, \quad r = 1, \quad H_*(K; \mathbb{F}_2) \cong H_*(\mathbb{R}P^2; \mathbb{F}_2), \quad H_*(X; \mathbb{F}_2) \cong H_*(S^2; \mathbb{F}_2).$$

This finishes the proof of Theorem 1.1 when X is path-connected. \square

7.2. When X is not path-connected.

In this case, it is possible that $b_1(K; \mathbb{F}_p) = 0$. So we have two cases.

- When $b_1(K; \mathbb{F}_p) = 0$, X is a trivial covering space over K , i.e. X is the disjoint union of 2^r copies of K . So

$$\text{hrk}(X; \mathbb{F}_p) = 2^r \cdot \text{hrk}(K; \mathbb{F}_p) \geq 2^r.$$

In particular, $\text{hrk}(X; \mathbb{F}_p) = 2^r \iff \text{hrk}(K; \mathbb{F}_p) = 1$, i.e. $H_*(K; \mathbb{F}_p) \cong H_*(pt; \mathbb{F}_p)$.

- When $b_1(K; \mathbb{F}_p) \geq 1$, there exists an $1 \leq s \leq r$ so that

- X has 2^s path components X_1, \dots, X_{2^s} which are pairwise homeomorphic. So $\text{hrk}(X; \mathbb{F}_p) = 2^s \cdot \text{hrk}(X_1; \mathbb{F}_p)$.
- Each component X_j of X is a regular $(\mathbb{Z}_p)^{r-s}$ -covering space of K . So by our discussion in the previous section, $\text{hrk}(X_j; \mathbb{F}_p) \geq 2^{r-s}$.

So we have $\text{hrk}(X; \mathbb{F}_p) = 2^s \cdot \text{hrk}(X_1; \mathbb{F}_p) \geq 2^s \cdot 2^{r-s} = 2^r$.

So we finish the whole proof of Theorem 1.1. \square

8. PROOF OF THEOREM 1.3 AND THEOREM 1.4

Let us only prove Theorem 1.3 and Theorem 1.4 when M is connected. If M is not connected, the proof follows easily from the connected case by the same argument as in Section 7.2.

Suppose we have a free $(\mathbb{Z}_p)^r$ -action on a compact connected 3-manifold M . Then the orbit space $M/(\mathbb{Z}_p)^r$ is also a compact connected 3-manifold, denoted by Q . The fundamental group of Q is finitely presentable. Let $\xi : M \rightarrow Q$ be the orbit map. Choose a basepoint $x_0 \in M$ and let $q_0 = \xi(x_0) \in Q$.

If M has boundary, so does Q . Since any compact connected 3-manifold with boundary is homotopy equivalent to a finite 2-dimensional CW-complex, so M is homotopy equivalent to a regular $(\mathbb{Z}_p)^r$ -covering over a finite 2-dimensional CW-complex. Then by Theorem 1.1, $\text{hrk}(M; \mathbb{F}_p) \geq 2^r$.

So in the rest of this section, we assume that M has no boundary, and so Q is a closed connected 3-manifold. The following well known result asserts that $\pi_1(Q, q_0)$ always admits a balanced presentation.

Theorem 8.1. *The fundamental group of any closed connected 3-manifold Q admits a balanced presentation. In fact, if Q possesses a Heegaard decomposition of genus k , then the fundamental group of Q can be presented by k generators and k defining relators.*

Indeed, suppose Q has a Heegaard decomposition of genus n . Then there is a canonical cell decomposition of Q associated to this Heegaard decomposition which consists of a single 0-cell, n 1-cells, n 2-cells and a single 3-cell. So the fundamental group $\pi_1(Q, q_0)$ has a presentation $\mathcal{P} = \langle a_1, \dots, a_n \mid R_1, \dots, R_n \rangle$ whose presentation complex is exactly the 2-skeleton of Q .

Since M is a regular covering space of Q with deck transformation group $(\mathbb{Z}_p)^r$, $\pi_1(M, x_0)$ can be thought of as a normal subgroup of $\pi_1(Q, q_0)$ with

$$\pi_1(Q, q_0)/\pi_1(M, x_0) \cong (\mathbb{Z}_p)^r.$$

So by the fact that $\pi_1(Q, q_0)$ admits a balanced presentation and Theorem 6.4,

$$\begin{aligned} b_1(M; \mathbb{F}_p) &= b_1(\pi_1(M, x_0); \mathbb{F}_p) \geq 1 + b_1(Q; \mathbb{F}_p) |\Omega_{p,r}^{\lfloor \frac{r(p-1)}{2} \rfloor}| - p^r \\ &\geq 1 + r |\Omega_{p,r}^{\lfloor \frac{r(p-1)}{2} \rfloor}| - p^r. \end{aligned} \quad (35)$$

Proof of Theorem 1.3. When $p = 2$, the inequality (35) reads

$$b_1(M; \mathbb{F}_2) \geq 1 + b_1(Q; \mathbb{F}_2) |\Omega_{2,r}^{\lfloor \frac{r}{2} \rfloor}| - 2^r \geq 1 + r \binom{r}{\lfloor \frac{r}{2} \rfloor} - 2^r. \quad (36)$$

In addition, $b_1(M; \mathbb{F}_2) = b_2(M; \mathbb{F}_2)$ by Poincaré duality. So to prove

$$\text{hrk}(M; \mathbb{F}_2) = 2 + b_1(M; \mathbb{F}_2) + b_2(M; \mathbb{F}_2) = 2 + 2b_1(M; \mathbb{F}_2) \geq 2^r,$$

we need to show $b_1(M; \mathbb{F}_2) \geq 2^{r-1} - 1$. Then by (36), it is sufficient to show

$$r \binom{r}{\lfloor \frac{r}{2} \rfloor} \geq 3 \cdot 2^{r-1} - 2. \quad (37)$$

But it turns out that the inequality in (37) holds if and only if $r \geq 4$ (we leave it as an exercise to the reader). So only when $r \geq 4$ can we use our method to prove $\text{hrk}(M; \mathbb{F}_2) \geq 2^r$. Note that the $r = 1$ case is trivial. But for $r = 2, 3$, our estimate of $b_1(M; \mathbb{F}_2)$ from Theorem 6.2 is insufficient! Fortunately, when $r \leq 3$, [24, Theorem 1.1] has already shown $\text{hrk}(M; \mathbb{F}_2) \geq 2^r$. So we have $\text{hrk}(M; \mathbb{F}_2) \geq 2^r$ for all $r \geq 1$.

Next, we discuss when $\text{hrk}(M; \mathbb{F}_2) = 2^r$. Notice that when $r \geq 4$, the inequality in (37) is always strict. So $\text{hrk}(M; \mathbb{F}_2) = 2^r$ implies $r \leq 3$ and $b_1(Q; \mathbb{F}_2) = r$ (see (35)). Then by the assumption $\text{hrk}(M; \mathbb{F}_2) = 2 + b_1(M; \mathbb{F}_2) + b_2(M; \mathbb{F}_2) = 2^r$, we get $b_1(M; \mathbb{F}_2) = b_2(M; \mathbb{F}_2) = 2^{r-1} - 1$. In addition, since Q is a closed connected manifold, we have $b_1(Q; \mathbb{F}_2) = b_2(Q; \mathbb{F}_2)$. All the possible cases are:

- $r = 1$, $b_2(Q; \mathbb{F}_2) = b_1(Q; \mathbb{F}_2) = r = 1$ and $b_1(M; \mathbb{F}_2) = b_2(M; \mathbb{F}_2) = 0$. So

$$H_*(Q; \mathbb{F}_2) \cong H_*(\mathbb{R}P^3; \mathbb{F}_2), \quad H_*(M; \mathbb{F}_2) \cong H_*(S^3; \mathbb{F}_2).$$

- $r = 2$, $b_2(Q; \mathbb{F}_2) = b_1(Q; \mathbb{F}_2) = r = 2$ and $b_1(M; \mathbb{F}_2) = b_2(M; \mathbb{F}_2) = 1$. So

$$H_*(Q; \mathbb{F}_2) \cong H_*(S^1 \times \mathbb{R}P^2; \mathbb{F}_2), \quad H_*(M; \mathbb{F}_2) \cong H_*(S^1 \times S^2; \mathbb{F}_2).$$

- $r = 3$, $b_2(Q; \mathbb{F}_2) = b_1(Q; \mathbb{F}_2) = r = 3$ and $b_1(M; \mathbb{F}_2) = b_2(M; \mathbb{F}_2) = 3$. So

$$H_*(Q; \mathbb{F}_2) \cong H_*(M; \mathbb{F}_2) \cong H_*(S^1 \times S^1 \times S^1; \mathbb{F}_2).$$

So Theorem 1.3 is proved. Note that all of the above three cases can be realized by concrete free actions of $(\mathbb{Z}_2)^r$ on some 3-manifolds. \square

Remark 8.2. In Theorem 1.3, if $p \neq 2$, we can not prove $b_1(M; \mathbb{F}_p) \geq 2^{r-1} - 1$ via our estimates in section 6. So some more accurate estimate of $b_1(M; \mathbb{F}_p)$ is needed to deal with those cases.

Proof of Theorem 1.4. Since we assume that the deficiency of the fundamental group $\pi_1(Q, q_0)$ of Q is at least 1, so in particular, $\pi_1(Q, q_0)$ admits a deficiency-1 presentation. Then by the fact $\pi_1(Q, q_0)/\pi_1(M, x_0) \cong (\mathbb{Z}_p)^r$ and Theorem 6.3, we can conclude that $b_1(M; \mathbb{F}_p) \geq 2^{r-1}$ and, only when $b_1(Q; \mathbb{F}_p) = r = 1$ or 2 can we have $b_1(M; \mathbb{F}_p) = 2^{r-1}$.

- If M is orientable, $\text{hrk}(M; \mathbb{F}_p) = 2 + 2b_1(M; \mathbb{F}_p) \geq 2^r + 2$.
- If M is not orientable,
 - $p = 2$, $\text{hrk}(M; \mathbb{F}_2) = 2 + 2b_1(M; \mathbb{F}_2) \geq 2^r + 2$.
 - $p \neq 2$, $\text{hrk}(M; \mathbb{F}_p) = 2b_1(M; \mathbb{F}_p) \geq 2^r$.

So in all cases, $\text{hrk}(M; \mathbb{F}_p) \geq 2^r$. In particular, $\text{hrk}(M; \mathbb{F}_p) = 2^r$ implies

- $b_1(M; \mathbb{F}_p) = 2^{r-1}$, so $r = 1$ or 2 ,
- $p \neq 2$, i.e. p is an odd prime,
- M is non-orientable, so Q is also non-orientable.

Then Q and M must be one the following cases:

- $r = 1$, $p \neq 2$, $b_1(Q; \mathbb{F}_p) = 1$, $b_2(Q; \mathbb{F}_p) = b_3(Q; \mathbb{F}_p) = 0$ and $b_1(M; \mathbb{F}_p) = 1$, $b_2(M; \mathbb{F}_p) = b_3(M; \mathbb{F}_p) = 0$. So

$$H_*(Q; \mathbb{F}_p) \cong H_*(M; \mathbb{F}_p) \cong H_*(S^1 \times \mathbb{R}P^2; \mathbb{F}_p) \cong H_*(S^1; \mathbb{F}_p).$$

- $r = 2$, $p \neq 2$, $b_1(Q; \mathbb{F}_p) = 2$, $b_2(Q; \mathbb{F}_p) = 1$, $b_3(Q; \mathbb{F}_p) = 0$ and $b_1(M; \mathbb{F}_p) = 2$, $b_2(M; \mathbb{F}_p) = 1$, $b_3(M; \mathbb{F}_p) = 0$. So

$$H_*(Q; \mathbb{F}_p) \cong H_*(M; \mathbb{F}_p) \cong H_*(S^1 \times \text{Klein Bottle}; \mathbb{F}_p) \cong H_*(S^1 \times S^1; \mathbb{F}_p).$$

So Theorem 1.4 is proved. Note that the above two cases can both be realized by concrete free actions of $(\mathbb{Z}_p)^r$ on some 3-manifolds. \square

9. AN APPLICATION

We use Theorem 6.3 to give a new proof of the following proposition in [20].

Proposition 9.1 ([20] Proposition 8.6). *Let G be a group with deficiency at least 1. Suppose that $b_1(H; \mathbb{F}_p) \geq 3$ for some finite index subgroup H of G . Then*

$$\sup\{b_1(G_i; \mathbb{F}_p) : G_i \text{ is a finite index subgroup of } G\} = \infty$$

Proof. Let $\gamma_2(H) = [H, H]H^p$. Then we have $H/\gamma_2(H) \cong (\mathbb{Z}_p)^{b_1(H; \mathbb{F}_p)}$. So by Theorem 6.3, we conclude that $b_1(\gamma_2(H); \mathbb{F}_p) \geq 2^{b_1(H; \mathbb{F}_p)-1} \geq 2^{3-1} = 4$. Repeating the argument for $\gamma_2(\gamma_2(H))$, and so on, we obtain a sequence $\{G_i\}$ of finite index subgroup of G , such that $b_1(G_i; \mathbb{F}_p)$ tends to infinity. \square

Remark 9.2. In the above statement, the hypothesis that the deficiency of G is at least 1 is necessary. For example, the deficiency of $G = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ is 0, but any finite index subgroup of G is isomorphic to $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$. In addition, the condition $b_1(H; \mathbb{F}_p) \geq 3$ can not be loosen either. For example, the deficiency of $\mathbb{Z} \oplus \mathbb{Z}$ is 1 and $b_1(\mathbb{Z} \oplus \mathbb{Z}, \mathbb{F}_p) = 2$, but any finite index subgroup of $\mathbb{Z} \oplus \mathbb{Z}$ is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$.

REFERENCES

- [1] A. Adem, \mathbb{Z}/p Actions on $(S^n)^k$, Transactions of the AMS **300** (1987), 791–809.
- [2] A. Adem and W. Browder, *The free rank of symmetry of $(S^n)^k$* , Invent. Math. **92** (1988), 431–440.
- [3] A. Adem and D. J. Benson, *Elementary abelian groups acting on products of spheres*, Math. Zeitschrift **228** (1998), 705–712.
- [4] A. Adem, *Constructing and deconstructing group actions*, Homotopy theory: relations with algebraic geometry, group cohomology, and algebraic K-theory, Contemp. Math., **346** (2004), 1–8.
- [5] C. Allday and V. Puppe, *Cohomological methods in transformation groups*, Cambridge University Press (1993).
- [6] A. Bak and G. Tang, *Solution to the presentation problem for powers of the augmentation ideal oftorsion free and torsion abelian groups*, Adv. Math. **189** (2004), 1–37.
- [7] X. Cao and Z. Lü, *Möbius transform, moment-angle complex and Halperin-Carlsson conjecture*, Preprint (2009); arXiv:0908.3174.
- [8] G. Carlsson, *On the rank of abelian groups acting freely on $(S^n)^k$* , Invent. Math. **69** (1982), 393–400.
- [9] G. Carlsson, *Free $(\mathbb{Z}/2)^k$ actions and a problem in commutative algebra*, Lecture Notes in Math., **1217**, Springer, Berlin, 1986, 79–83.
- [10] G. Carlsson, *Free $(\mathbb{Z}/2)^3$ Actions on Finite Complexes*, Annals of Math. Studies 113 (1987), 332–344.
- [11] S. Choi, M Masuda and S. Oum, *Classification of real Bott manifolds and acyclic digraphs*, arXiv:1006.4658.
- [12] D. J. Collins and H. Zieschang, *Combinatorial group theory and fundamental groups*, Algebra, VII, 1–166, 233–240, Encyclopaedia Math. Sci., **58**, Springer, Berlin, 1993.
- [13] I. G. Connell, *On the group ring*, Canad. J. Math. **12** (1963), 650–685.
- [14] P. E. Conner, *On the action of a finite group on $S^n \times S^n$* , Ann. of Math. **66** (1957), 586–588.
- [15] Y. Félix, J. Oprea and D. Tanré, *Algebraic Models in Geometry*, Oxford University Press, 2008.
- [16] S. Halperin, *Rational homotopy and torus actions. Aspects of topology*, 293–306, London Math. Soc. Lecture Note Ser., **93**, Cambridge Univ. Press, Cambridge, 1985.
- [17] B. Hanke, *The stable free rank of symmetry of products of spheres*, Invent. Math. **178** (2009), no. **2**, 265–298.

- [18] S. A. Jennings, *The structure of the group ring of a p -group over a modular field*, Trans. Amer. Math. Soc. **50** (1941), 175–185.
- [19] Y. Kamishima and M. Nakayama, *Torus actions and the Halperin-Carlsson Conjecture*, arXiv:1206.4790.
- [20] M. Lackenby, *New lower bounds on subgroup growth and homology growth*, Proc. London Math. Soc. 98 (2009) No. 3, 271–297.
- [21] C. Polcino Milies and S. K. Sehgal, *An introduction to group rings, Algebras and Applications*, 1, Kluwer Academic Publishers, Dordrecht, 2002.
- [22] I. B. S. Passi, *Group rings and their augmentation ideals*, Lecture Notes in Mathematics **715**, Springer, Berlin, 1979.
- [23] M. M. Parmenter, *A basis for powers of the augmentation ideal*, Algebra Colloq. 8 (2001), no. **2**, 121–128.
- [24] V. Puppe, *Multiplicative aspects of the Halperin-Carlsson conjecture*, Georgian Math. J. 16 (2009), no. **2**, 369–379.
- [25] G. Tang, *Structure of augmentation quotients of finite homocyclic abelian groups*, Sci. China Ser. A 50 (2007), no. **9**, 1280–1288.
- [26] S. Chang and G. Tang, *A basis for augmentation quotients of finite abelian groups*, J. Algebra **327** (2011), 466–488.
- [27] Y. M. Ustinovskii, *Toral rank conjecture for moment-angle complexes*, Mathematical Notes Vol. 90 (2011) No. 2, 279–283.
- [28] L. Yu, *Small Covers and Halperin-Carlsson Conjecture*, Pac. J. Math., Vol. **256** (2012) No. **2**, 489–507.

DEPARTMENT OF MATHEMATICS AND IMS, NANJING UNIVERSITY, NANJING, 210093,
P.R.CHINA

E-mail address: yuli@nju.edu.cn